PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-357365

(43)Date of publication of application : 26.12.2001

---

(51)Int.Cl. G06K 17/00

G06K 19/07

G06K 19/00

G09C 1/00

---

(21)Application number : 2000-180051 (71)Applicant : SONY CORP

(22)Date of filing : 15.06.2000 (72)Inventor : SHIRAI TAIZO

ISHIBASHI YOSHITO

ASANO TOMOYUKI

YOSHINO KENJI

OKA MAKOTO

TAKI RYUTA

---

(54) DATA STORAGE, DATA STORAGE METHOD AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To ensure security and also to simultaneously receive supply of plural types of services with a single IC card.

SOLUTION: The data which permit access to the service data on another type of service while a certain type of service is performed are registered on a service relation table when plural types of service are registered on an IC card. The service relation table includes a registered service ID field where the service IDs registered on the IC card are described and a permission information field where the permission information corresponding to each service ID is described. The

permission information describes a service ID that can be accessed when its corresponding service is performed and the information that shows the executable processing to the accessible service ID.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the data storage with which an information processor is equipped and which performs transfer of said information processor and data An input/output control means against said information processor to control I/O of said data, The 1st storage control means which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of the services of said plurality When I/O of said data about said 1st service is controlled by said input/output control means, I/O of said data is permitted. Data storage characterized by having the 2nd storage control means which controls storage of the 2nd service ID corresponding to the 2nd service of the services of said plurality.

[Claim 2] Said 2nd storage control means is data storage according to claim 1 characterized by controlling further storage of the information about a limit of the

access privilege about said 2nd service.

[Claim 3] Said 2nd storage control means is data storage according to claim 1 characterized by controlling storage of two or more 2nd services ID of said when two or more said 2nd service ID exists to said 1st service ID, and controlling storage so that said 2nd service ID serves as a blank when one does not exist [said 2nd service ID] to said 1st service ID.

[Claim 4] In the data store method of the data storage with which an information processor is equipped and which performs transfer of said information processor and data The input/output control step to said information processor which controls I/O of said data, The 1st storage control step which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of the services of said plurality When I/O of said data about said 1st service is controlled by processing of said input/output control step, I/O of said data is permitted. The data store method characterized by including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of the services of said plurality.

[Claim 5] The input/output control step which an information processor is equipped with, and is a program said information processor and for the data storage which performs transfer of data, and controls the I/O of said data to said information processor, The 1st storage control step which controls the data

storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of the services of said plurality When I/O of said data about said 1st service is controlled by processing of said input/output control step, I/O of said data is permitted. The record medium with which the program which the computer characterized by including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of the services of said plurality can read is recorded.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the data storage and the data store method which make it possible to perform in parallel transfer of the data about other services permitted beforehand, securing security, when the IC card and the reader writer are performing transfer of the data about predetermined service concerning data storage and a data store method.

[0002]

[Description of the Prior Art] Use of IC (Integrated circuit) card is increasing in a

cybermoney system and a security system. The IC card contains the memory which memorizes CPU (Central Processing Unit) which performs various processings, data required for processing, etc., and transmission and reception of data are performed by non-contact using the condition of having made the predetermined reader writer contacting electrically, or an electromagnetic wave. In addition, generally required power is supplied to the IC card transmit and receive data by non-contact between reader writers using an electromagnetic wave by the electromagnetic wave.

[0003] A common key system or a public key system is used for an IC card and authentication of a reader writer. The key used for decode is the same as the key used for encryption in a common key system. Since it is necessary to share a common key between a transmitting person and an addressee beforehand in order to use a common key encryptosystem, it is necessary to send the key used for encryption to a communications partner using safe means by which a channel is another (that is, the IC card and the reader writer must share the common key beforehand). Fundamentally, encryption is performed combining the "substitution" which transposes "the transposition (character transposition)" which replaces the sequence of an alphabetic character, and the alphabetic character according to a fixed regulation to another alphabetic character. Cryptographic algorithm and a key show in what kind of sequence it changes, or

which alphabetic character and which alphabetic character are replaced. In encryption, the number of alphabetic characters which the transposition code for changing the substitution cipher for shifting an alphabetic character and the sequence of an alphabetic character is fundamental code conversion, and is shifted serves as a key.

[0004] In a code system, the two keys an "encryption key" and a "decode key" are used for a public key system in a pair, the encryption key of them is exhibited, the publisher of a key manages a decode key and it is made secret. When transmitting data, correspondence is enciphered using an encryption key and it returns using a decode key in the side which received. Although it is not impossible to ask for a decode key from an encryption key since two keys are decided based on a certain mathematical relation, it is not realistic from the point of computational complexity.

[0005] Although it has the advantage of it not being necessary to distribute a decode key and having the authentication function of the message by the digital signature further since a public key cryptosystem should just have even the decode key which each user has separately in order distribution of an encryption key is easy and to decode a cipher, since it is not necessary to keep an encryption key secret compared with the conventional common key encryptosystem system, compared with a common key encryptosystem system,

the time amount concerning authentication processing becomes long.

[0006] A digital signature is an approach to show that it is sent by the addresser with the just message, and the alteration etc. is not performed on the way in an electronic mail, online dealings, etc. In the usual cipher communication link, although it enciphers with a public key, in the case of a RSA (Rivest, Shamir, Adleman) public key cryptosystem, it is "Enciphering with a decode key (private key)" with a digital signature conversely, for example. Moreover, in other cipher systems, to data to add a signature, the hash value was taken and it is enciphered with the private key.

[0007] A public key is used in order to verify this signature (that is, the role of an encryption key and a decode key is replaced). Since the public key is exhibited widely, anyone can inspect the justification of the signature easily. A public key can restore a cipher correctly, and if a meaningful sentence is obtained, it can be checked as he is a right addresser. Only the addresser of normal knows the private key (key which signed), and in order to create the digital signature which can be restored with a public key, it is because the private key used as the pair must be known. Moreover, when data are altered, since it becomes impossible to decode data correctly, they are applicable also to prevention and detection of an alteration. If verification of a signature is performed by comparing the value decoded using the public key with the hash value separately recalculated from

data, and is in agreement and it is not [it is judged that data are not altered and] in agreement, it is judged that the alteration of data was performed.

[0008] Moreover, the organization of the 3rd person aiming at publishing the certificate for proving that he is the organization for which data issue-origin can set reliance is called certificate authority (CA (Certificate Authority)).

[0009]

[Problem(s) to be Solved by the Invention] Other services cannot be received while having received one service, when receiving two or more services conventionally using an IC card. In an IC card and a reader writer, it is because it is necessary to perform authentication processing in order to deliver and receive predetermined data and to secure the security to each data. However, when prepaid service and cybermoney service can be received for example, using the same reader writer as the same IC card, there is a demand of wanting to be filled up with cybermoney, performing liquidation processing about prepaid service.

[0010] It makes it possible to perform in parallel transfer of the data about other services permitted beforehand, securing security, when this invention is made in view of such a situation and transfer of the data about predetermined service is being performed.

[0011]

[Means for Solving the Problem] An input/output control means as opposed to an

information processor in the data storage of this invention and to control I/O of data, The 1st storage control means which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of two or more services When I/O of the data about the 1st service is controlled by the input/output control means, it is characterized by having the 2nd storage control means which controls storage of the 2nd service ID corresponding to the 2nd service of two or more services to which I/O of data is permitted.

[0012] The 2nd storage control means can be made to control storage of the information about a limit of the access privilege about the 2nd service.

[0013] When two or more 2nd service ID exists to the 1st service ID, storage of two or more 2nd services ID is made to control, and the 2nd storage control means can be made to control storage so that the 2nd service ID serves as a blank when one does not exist [the 2nd service ID] to the 1st service ID.

[0014] The input/output control step by which the data store method of this invention controls the I/O of data to an information processor, The 1st storage control step which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of two or more services I/O of data is permitted when I/O of the data about the 1st service is controlled by processing of an input/output control step. It is characterized by

including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of two or more services.

[0015] The program currently recorded on the record medium of this invention The input/output control step to an information processor which controls I/O of data, The 1st storage control step which controls the data storage corresponding to two or more services, The 1st service ID corresponding to the 1st service of two or more services I/O of data is permitted when I/O of the data about the 1st service is controlled by processing of an input/output control step. It is characterized by including the 2nd storage control step which controls storage of the 2nd service ID corresponding to the 2nd service of two or more services.

[0016] In the program currently recorded on the data storage, data store method, and record medium of this invention The 1st service ID corresponding to [I/O of the data to an information processor is controlled, and the data storage corresponding to two or more services is controlled, and] the 1st service of two or more services When I/O of the data about the 1st service is controlled by processing of an input/output control step, storage of the 2nd service ID corresponding to the 2nd service of two or more services to which I/O of data is permitted is controlled.

[0017]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention

is explained with reference to drawing.

[0018] The relation between an IC card and a reader writer is shown in drawing 1 . IC card 1 can be dealt with authentication service of both authentication by the common key system, and the authentication by the public key system (about each authentication approach, it mentions later). The reader writer 2-1 corresponding to a non-contact type common key communicates by IC card 1 and non-contact, and attests with a common key system. The reader writer 2-2 corresponding to a non-contact type public key communicates by IC card 1 and non-contact, and attests with a public key system. The reader writer 2-3 corresponding to a contact process public key communicates by contacting, and communicates with a public key system.

[0019] For example, the information which offers service of the prepaid card which can perform payment of a commuter pass or a fare is included in IC card 1. To the case where the ticket gate of a station is used using IC card 1, and IC card 1 The function as an ID card is included and the non-contact communication link with a common key is performed using the reader writer 2-1 corresponding to a non-contact type common key in the processing asked for the short processing times in the case of attesting entrance authorization using IC card 1 etc.

[0020] For example, the information which offers service of cybermoney is

included in IC card 1, when processing liquidation of the goods which the user purchased at the store etc., authentication is performed by the public key system and authentication processing takes time amount. For this reason, when not caring especially about the processing time, in order to communicate by non-contact and to shorten the processing time using the reader writer 2-2 corresponding to a non-contact type public key, the reader writer 2-3 corresponding to a contact process public key is used, and it may be made to communicate by contacting.

[0021] Although the reader writer 2-1 thru/or the reader writer 2-3 corresponding to a contact process public key corresponding to a non-contact type common key is explained as a reader writer according to individual, it is one reader writer and you may enable it to use two or more correspondence procedures and two or more authentication approaches in drawing 1 if needed.

[0022] Next, a card publisher, a service provider, and a card holder are explained using drawing 2 .

[0023] The card publisher 11 approves providing a service provider 12 with the service using IC card 1 to the card holder 13 who holds IC card 1, and publishes IC card 1 to the card holder 13 who wished issue of IC card 1.

[0024] From the card publisher 11, the service provider 12 which received license of service registers the data (Service Individual Info later mentioned

using drawing 6) corresponding to the service with which he provides the card holder 13 into the reader writer 2-11 for service registration which the card publisher 11 has. You may make it register with the reader writer 2-11 for service registration, and an operator may be made to register manually through the Internet etc. about this registration from the personal computer which a service provider 12 has and which is not illustrated, for example.

[0025] The card holder 13 can make it register into IC card 1 published by the card publisher 11 using the reader writer 2-11 for service registration to give [to wish one's service]. About the reader writer 2-11 for service registration, and service registration processing of IC card 1, it mentions later using drawing 29 and drawing 30 .

[0026] And the card holder 13 can make service delete from its own IC card 1 using the reader writer 2-11 for service registration which the card publisher 11 manages, or the general reader writer 2-12 which a service provider 12 manages to delete service registered into its own IC card 1. About the service deletion of IC card 1 and the reader writer 2-11 for service registration, it mentions [deletion / of drawing 31 and drawing 32 , IC card 1, and the general reader writer 2-12 / service] later using drawing 33 and drawing 34 .

[0027] Moreover, cybermoney service and prepaid service are registered into IC card 1, and the card holder 13 is in the situation that each value information is

recorded on the information about each service of IC card 1. When you want to transpose a part of worth of cybermoney to prepaid value, Intermodule communication can be performed using the reader writer 2-13 for intermodule communications which a service provider 12 manages between the public key module later mentioned using drawing 13 of its own IC card 1, and a common key module. The reader writer 2-13 for intermodule communications is made as [correspond / to a common key system and two methods of a public key system]. About processing with IC card 1 and the reader writer 2-13 for intermodule communications, it mentions later using drawing 48 thru/or drawing 51 .

[0028] Furthermore, the card holder 13 can make the authentication key registered into its own IC card 1 upgrade using the general reader writer 2-12 which a service provider 12 manages, or the reader writer 2-14 for version up to update the invalidated authentication key (version up). About key version up processing with IC card 1 and the reader writer 2-14 for version up, it mentions [processing / with IC card 1 and the general reader writer 2-12 / key version up] later using drawing 45 thru/or 47 using drawing 43 and 44.

[0029] Drawing 3 is the block diagram showing the configuration of IC card 1.

[0030] IC card 1 consists of the communications department 21 which performs the communication link with the reader writer 2 (these shall be named

generically and the reader writer 2 shall be called about the case where there is no need of distinguishing the reader writer 2-1 thru/or 2-3 or the reader writer 2-11 thru/or especially 2-14), and the IC card processing section 22 which performs data processing.

[0031] The communications department 21 has the coil for communicating with the reader writer 2-1 corresponding to a non-contact type common key, or the reader writer 2-2 corresponding to a non-contact type public key using an electromagnetic wave, when corresponding IC card 1 is the reader writer 2-1 corresponding to the non-contact type common key explained using drawing 1 , or the reader writer 2-2 corresponding to a non-contact type public key. moreover, IC card 1 the communications department 21 only not only in the reader writer 2-1 corresponding to the non-contact type common key explained using drawing 1 , and the reader writer 2-2 corresponding to a non-contact type public key When the communication link with the reader writer 2-3 corresponding to a contact process public key is also supported, the reader writer 2-1 corresponding to a non-contact type common key, or the reader writer 2-2 corresponding to a non-contact type public key, It has the coil for communicating using an electromagnetic wave, and the contact terminal for communicating with the reader writer 2-3 corresponding to a contact process public key.

[0032] The communications department 21 receives the data transmitted from

the reader writer 2, and the received data When becoming irregular using ASK (Amplitude Shift Keying) or BPSK (Binary Phase Shift Keying), for example, by predetermined processing While restoring to the received data and supplying the control section 31 of the IC card processing section 22, the data generated by processing of the IC card processing section 22 are supplied from a control section 31, and it becomes irregular using ASK or BPSK, and transmits to the reader writer 2.

[0033] The IC card processing section 22 consists of a control section 31, memory 32, and the cipher-processing section 33. According to the data supplied from the communications department 21, a control section 31 controls the cipher-processing section 33, cipher processing required for authentication processing with the reader writer 2 etc. is performed, or it reads the data currently recorded on memory 32 if needed, and transmits to the reader writer 2 through the communications department 21.

[0034] Memory 32 consists of a memory area 44 where CA_Pub which is Card ID, the authentication key Kreg for service registration, and the public key of a certificate authority is recorded, Service Relation Table (SRT)45 later mentioned using drawing 8 , and Service Registration Area (SRA)46 later mentioned using drawing 6 .

[0035] The cipher-processing section 33 consists of the public key processing

section 41, the common key processing section 42, and the other cipher-processing sections 43. The detail about the processing which the public key processing section 41 thru/or the other cipher-processing sections 43 perform is later mentioned using drawing 5 .

[0036] Next, drawing 4 is the block diagram showing a different configuration from drawing 3 of IC card 1. In addition, in IC card 1 of drawing 4 , the same sign is given to the case in drawing 3 , and the corresponding part, and the explanation is omitted suitably (following, the same).

[0037] IC card 1 consists of the public key service processing sections 54 which perform processing of the data obtained by processing of the communications department 51 which performs the communication link with the reader writer 2 about common key service, the common key service processing section 52 which performs processing of the data obtained by processing of the communications department 51, the communications department 53 which performs the communication link with the reader writer 2 about public key service, and the communications department 53.

[0038] The communications department 51 has the coil for communicating with the reader writer 2-1 corresponding to a non-contact type common key. When the data transmitted from IC card 1 are modulated like the communications department 21 using ASK or BPSK, by predetermined processing While

restoring to the received data and supplying the control section 61 of the common key service processing section 52, the data generated by processing of the common key service processing section 52 are supplied from a control section 61, and it becomes irregular using ASK or BPSK, and transmits to the reader writer 2.

[0039] The common key service processing section 52 consists of a control section 61, memory 62, and the cipher-processing section 63. According to the data supplied from the communications department 51, a control section 61 controls the cipher-processing section 63, processing required for authentication processing with IC card 1 etc. is performed, or it reads the data currently recorded on memory 62 if needed, and transmits to the reader writer 2 through the communications department 51.

[0040] Memory 62 consists of a memory area 44, and SRT45 and SRA46 like the memory 32 explained using drawing 3 . Share private key K_common used by the authentication key Kreg and intermodule communication Card ID and for service registration is recorded on the memory area 44.

[0041] The cipher-processing section 63 consists of the common key processing section 42 and the other cipher-processing sections 43. That is, in the common key service processing section 52, in order not to process the service about a public key, the cipher-processing section 63 is not equipped with the public key

processing section 41 explained using drawing 3 .

[0042] The communications department 53 has the coil or contact terminal for communicating with the reader writer 2-2 corresponding to a non-contact type public key, or the reader writer 2-3 corresponding to a contact process public key. When the data with which the communications department 53 is also transmitted from IC card 1 are modulated using ASK or BPSK, like the communications department 21 by predetermined processing While restoring to the received data and supplying the control section 61 of the public key service processing section 54, the data generated by processing of the public key service processing section 54 are supplied from a control section 61, and it becomes irregular using ASK or BPSK, and transmits to the reader writer 2.

[0043] The public key service processing section 54 consists of a control section 61, memory 62, and the cipher-processing section 33. That is, except that it has the cipher-processing section 33 explained using drawing 3 instead of the cipher-processing section 63, it is the same configuration fundamentally with the common key service processing section.

[0044] Next, the public key processing section 41 thru/or the other cipher-processing sections 43 are explained using drawing 5 .

[0045] As shown in drawing 5 (A), the public key processing section 41 is equipped with RSA signature generation / verification section 71 which performs

generation and verification of a signature using a RSA (Rivest, Shamir, Adleman) public key cryptosystem, and DSA signature generation / verification section 72 which performs generation and verification of a signature using a DSA (Digital Signature Algorithm) method.

[0046] In RSA signature generation / verification section 71, two keys perform encryption and decode. In a RSA cryptosystem, two keys are decided as follows, for example.

[0047] Some two big prime factors p and q are chosen, and the product n=pq is calculated. And x (p-1) (q-1) and the relatively prime integer e are chosen below by x (p-1) (q-1), and the integer d with which the following formula (1) is filled is searched for.

Exd = 1 mod ... (x (p-1) (q-1)) (1)

Then (e, n), a public key and d become a private key.

[0048] When enciphering Sentence M and generating the encryption data C, the following formula (2) is used.

C=M e mod n ... (2)

Moreover, when decoding the encryption data C, the following formula (3) is used.

M=C d mod n ... (3)

[0049] DSA signature generation / verification section 72 is equipped with the

random-number generation section which is not illustrated. DSA is a digital signature algorithm which improves the ElGamal signature which used the difficulty of DLP (Discrete Logarithm Problem; dispersion a logarithm problem) as the base, shortens the die length of a signature to 160bitx2, and employs generation of a signature key etc. by the specific approach. It is premised on using SHA-1 (Secure Hash Algorithm-1) for a Hash Function (data compression function) in signature generation. The DSA method was developed as a criterion of electronic signature by NIST (U.S. Department of Commerce standard technical station: National Institute of Standards and Technology) which is the U.S. Government engine, and was set to U.S. Federal Information Processing Standard (Federal Information Processing Standard) FIPS PUB 186.

[0050] Moreover, as shown in drawing 5 (B), the common key processing section 42 is equipped with the DES processing section 73 which performs authentication processing by the DES (Data Encryption Standard) common key encryptosystem system, RC5 processing section 74 which performs authentication processing by RC5 (Rivest Cipher5) method, and the AES processing section 75 which performs authentication processing by the AES (Advanced Encryption Standard) method.

[0051] A DES common key encryptosystem system is a common key encryptosystem system which was enacted in NIST in 1977 and standardized by

American National Standards Institute (ANSI:American National Standards Institute) in 1981. The authentication algorithm of the key of a DES common key encryptosystem system is exhibited, and has spread widely as a representative of a common key encryptosystem system.

[0052] A DES common key encryptosystem system is a code system which divides data per 64 bits and performs encryption and decode processing. In a DES algorithm, encryption and decode are making the symmetry, and if the received cipher is changed once again using the same key, they can restore the original text. Moreover, in the DES common key encryptosystem system, the combination logic of easy bit-position transposition and an XOR operation is repeated 16 times. Since processing is successive, if there are no feedback and conditional-judgment part of data internally, and it pipelines, it can process at a high speed. It is the algorithm decided on the assumption that it LSI-ized from the first, and many DES chips are also made.

[0053] In RC5, it is the common key encryption system of RSA Data Security and RC series which Massachusetts Institute of Technology developed, and was proposed in 1995. RC5 is a block cipher system which has a variable-length block size, variable-length key size, and the round of the count of variable length (Data dependent rotations (data dependence bit rotation) algorithm which changes the amount of bit rotation with former data or a key). As the block size, it

is possible to take 32 or 64,128 bits, the number of rounds is 0 to 255, and key size is adjustable to 0 to 2048 bits. It is possible for the algorithm of RC5 to be exhibited and to receive as RFC2040.

[0054] Moreover, an AES method is a next-generation standard cipher system of the U.S. Government with which selection is performed by NIST. It is that DES used as a current standard code was enacted, and the dependability is falling every year with high-performance-izing of a computer in recent years, and development of the code theory. Then, NIST sought the cipher system which serves as an AES candidate from the whole world as a code criterion of the next generation replaced with DES. The method of 15 which gathered from all over the world is undergoing the examination, and is due to be determined by the beginning of the 21st century.

[0055] And to a message, it is making an irreversible Hash Function act, and the other cipher-processing sections 43 perform cipher processing except the public key processing section 41 or the common key processing section 42 of creating a digital signature processing by creating a "message digest" and enciphering a message digest with a signature key, when using a digital signature. In the other cipher-processing sections 43, as shown in drawing 5 (C) For example, [whether it has the SHA-1 processing section 76 which processes Hash Function SHA-1 used for signature generation and signature verification, and the

intrinsic random-number generation section 77 which generates the intrinsic random number used with a mutual recognition protocol, and] Or as shown in drawing 5 (D) The MD5 processing section 78 which processes Hash Function MD5 used for signature generation and signature verification, and the pseudo-random number (artificial random number which has the random possible digit string in the range of the figure of the existing limited digit count) used with a mutual recognition protocol It has the pseudo-random-number generation section 79 to generate.

[0056] In a digital signature, although that processing speed is slow poses a problem in order to use a public key cryptosystem, the time amount concerning digital signature creation is reduced by creating a message digest. Furthermore, since the Hash Function has the property of reacting greatly to the alteration of data, in case it verifies a digital signature, it can check easily whether the message body is altered by comparing the message digest which decoded and took out the digital signature with the verification key with the message digest which the Hash Function was made to act on the sent message body, and was created.

[0057] SHA-1 is an one-way hash function which generates the hash value of 160 bits from the message of the die length of arbitration. Like DSA, it is what NIST developed and is FIPS PUB180 by NIST. It was set. Standard draft

proposal (N544) is what was fundamentally based on FIPS PUB 180.

[0058] And MD5 is one of the message digest function algorithms currently generally used widely, and is defined by RFC1321. The algorithm is decided so that MD5 can be efficiently calculated on a 32-bit computer. There is also another similar algorithm [say / MD4 or MD2].

[0059] Next, the information stored in SRA46 of IC card 1 explained using drawing 3 and drawing 4 is explained using drawing 6 .

[0060] SRA46 is a memory area for recording the information (information registered using the reader writer 2-11 for service registration explained using drawing 2) for receiving those services of two or more, in order that the user who holds IC card 1 may enable it to receive two or more services using the general reader writer 2-12 explained using drawing 2 .

[0061] Namely, Service Individual Info1 thru/or N which is the information on the service registered into the IC card 1 is registered into SRA46. In each Service Individual Info Were beforehand set for every service ID for identifying the class of service, and service. One or two or more key information for authentication (in Service Individual Info k in drawing 6) The certificate to an authentication key etc. is registered if needed with authentication key Kake_vup for upgrading the service data used in order to receive 1 thru/or the key information for n authentications on n, and service, and key information.

[0062] The authentication key Kake for discernment (certificate [as opposed to an authentication key according to the need]) used in order to identify the level of for example, the authentication key ID and a key and a version, an authentication method, and two or more authentication keys is contained in the key information for authentication. Moreover, in addition to user ID, when Service Individual Info k is for example, cybermoney service, and Service Individual Info k, such as balance information, the accumulation point, etc. of cybermoney, is for example, automatic wicket services, effective section information etc. is stored in service data.

[0063] Next, the key information for authentication registered into Service Individual Info of drawing 6 is explained using drawing 7 .

[0064] In drawing 7 (A), certificate data are registered the version of the authentication key ID and a key, an authentication method, the authentication key Kake for discernment, and if needed corresponding to each of field No.1 and field No.2. About authentication key discernment processing in case the key information for authentication is registered like drawing 7 (A), it mentions later using drawing 20 thru/or drawing 24 .

[0065] In drawing 7 (B), certificate data are registered the level of the authentication key ID and a key, the version of a key, an authentication method, the authentication key Kake for discernment, and if needed corresponding to

each of field No.1 thru/or field No.7. About authentication key discernment processing in case the key information for authentication containing the level of a key is registered like drawing 7 (B), it mentions later using drawing 27 and drawing 28 .

[0066] Next, the information stored in SRT45 of IC card 1 explained using drawing 3 and drawing 4 is explained using drawing 8 .

[0067] When two or more services are registered into ID card 1 by SRT45, the data for permitting access to the service data of another service are registered into it, offering a certain service. SRT45 consists of a registration service ID field (drawing 8 is indicated as services IDA and J) the service ID registered into IC card 1 is indicated to be, and permission information field where the permission information corresponding to each service ID is indicated.

[0068] The services ID of the service registered are altogether enumerated by the registration service ID field of permission information. And when corresponding service is performed, the information which shows what kind of processing [the service ID which can access the service indicated by the registration service ID field, and] it permits are performed is indicated in permission information field. For example, when read-out and writing are permitted, "rw" is indicated as permission information, when only read-out is permitted, "ro" is indicated as permission information, and when version up of a

key is permitted, "vup" is indicated as permission information. Although "rw" and "ro" are not permitted to the same service ID, a permission is granted to the same service ID and "rw", "vup", and "ro" and "vup" can be enumerated to permission information field.

[0069] namely, when the permission information shown in drawing 8 is registered into SRT45, during activation of the service Service ID is indicated to be by C It is also under [activation / of the service with which read, and writing is permitted to the service Service ID is indicated to be by B, and Service ID is further indicated to be by D] also setting. As opposed to the service Service ID is indicated to be by D during activation of the service with which read-out to the service Service ID is indicated to be by B is permitted, and Service ID is indicated to be by E Read-out, writing, and version up of a key are permitted. The following, the service Service ID is indicated to be by E, the service Service ID is indicated to be by F, and the service Service ID is indicated to be by G -- or Also in the service Service ID is indicated to be by I, the processing corresponding to permission information is permitted during activation of the processing corresponding to other services ID based on the information indicated in corresponding permission information field.

[0070] Registration of such permission information is performed when registering the service corresponding to IC card 1. Namely, a user receives IC

card 1 which he holds using the reader writer 2-11 for service registration. If the service Service ID is indicated to be by G is already registered and the service Service ID is indicated to be by H is not registered when registering the service Service ID is indicated to be by F for example Only the permission information corresponding to the service Service ID is indicated to be by G can be registered into the permission information field corresponding to F of a registration service ID field. And after a user registers into ID card 1 the service Service ID is indicated to be by H, the permission information on service over the service Service ID is indicated to be by F by which Service ID is shown by H can be registered by updating the service Service ID is indicated to be by F.

[0071] Next, drawing 9 is the block diagram showing the configuration of the reader writer 2.

[0072] The reader writer 2 consists of the communications department 91 which performs the communication link with IC card 1, and the reader writer processing section 92 which performs data processing.

[0073] The communications department 91 has structure equipped with the contact terminal for communicating by the coil for having only a coil for namely, communicating using an electromagnetic wave by whether the reader writer 2 has adopted which communication mode of the non-contact type explained using drawing 1 , and a contact process, or communicating by the

correspondence procedure with IC card 1, using an electromagnetic wave, and the contact process.

[0074] When the communications department 91 receives the data transmitted from IC card 1 and the received data are modulated using ASK or BPSK, by predetermined processing While restoring to the received data and supplying the control section 101 of the reader writer processing section 92, the data generated by processing of the reader writer processing section 92 are supplied from a control section 101, and it becomes irregular using ASK or BPSK, and transmits to IC card 1.

[0075] The reader writer processing section 92 consists of a control section 101, the cipher-processing section 102, memory 103, the communications department 104, a display 105, and the input section 106. A control section 101 controls the cipher-processing section 102 according to the data supplied from the communications department 91, and the data currently recorded on memory 103 are read if needed in performing cipher processing required for authentication processing with IC card 1 etc. ****. The signal corresponding to the various actuation which the user inputted, using the input section 106 in transmitting to IC card 1 ****, and a network are minded through the communications department 91. The input of the control signal inputted into the communications department 104 is received, processing is performed according

to these signals, and the result is displayed on a display 105.

[0076] moreover, transfer of the magnetic disk 115 with which the drive 114 is also connected to the communications department 104, and drive 114 is equipped, an optical disk 116, a magneto-optic disk 117 semiconductor memory 118, etc. and data -- a line -- things are made.

[0077] Since it has the same configuration as the cipher-processing section 33 explained using drawing 3 , the cipher-processing section 102 omits the explanation.

[0078] The information for performing processing of IC card 1 and predetermined is memorized by memory 103. The information differs by the thing corresponding to any of the reader writer 2-11 for service registration explained using drawing 2 thru/or the reader writer 2-14 for version up the reader writer 2 is. The data memorized by the memory 103 of the reader writer 2-11 for service registration thru/or the reader writer 2-14 for version up are explained using drawing 10 thru/or drawing 14 .

[0079] The authentication key Kreg used for the memory 103 of the reader writer 2-11 for service registration shown in drawing 10 when registering or deleting data to SRA46 of the memory 32 of IC card 1 is memorized (the certificate of an authentication key is also memorized if needed), and Service Individual Info1 thru/or n corresponding to the various services for registering with IC card 1 is

memorized.

[0080] The service ID corresponding to the service which can be processed by this general reader writer 2-12, the authentication key list corresponding to it, and key lapse information are memorized by the memory 103 of the general reader writer 2-12 shown in drawing 11 . Moreover, when making the general reader writer 2-12 enable service of key version up, the information on the key of an upgrade product etc. is also united and memorized by the memory 103 of the general reader writer 2-12 at it.

[0081] The service ID corresponding to the service which can be processed by this reader writer 2-13 for intermodule communications, the authentication key list corresponding to it, and key lapse information as well as the information memorized by the memory 103 of the general reader writer 2-12 are memorized by the memory 103 of the reader writer 2-13 for intermodule communications shown in drawing 12 . As indicated in drawing 13 as intermodule communication, to the reader writer 2-13 for intermodule communications currently made as [correspond / to two methods of a common key system and a public key system] The public key module 121 (for example, it corresponds to the communications department 53 of IC card 1 which explained using drawing 4 , and the public key service processing section 54), It equips with IC card 1 which has the common key module 122 (for example, it corresponds to the

communications department 51 of IC card 1 explained using drawing 4 , and the common key service processing section 52). It is performing the communication link of the data of the public key module 121 and the common key module 122 through the reader writer 2-13 for intermodule communications. The detail of the processing about intermodule communication is later mentioned using drawing 48 thru/or drawing 51 .

[0082] And the list of authentication key Kake_vup for version up corresponding to Service ID and its service ID and the authentication keys Kake for upgrading the authentication key of the service registered into IC card 1 with which it was equipped to the memory 103 of the reader writer 2-14 for version up shown in drawing 14 is memorized.

[0083] When IC card 1 and the reader writer 2 communicate, in order for the reader writer 2 to carry out mutual recognition to IC card 1 first except for processing used as some exceptions, it is necessary to identify the service which communicates mutually and to identify the authentication key of the service mutually. With reference to the flow chart of drawing 15 , mutual recognition processing of IC card 1 and the reader writer 2 is explained.

[0084] First, in step S1, the reader writer 2 performs service discernment processing of the reader writer 2 later mentioned using drawing 16 and drawing 18 by communicating with IC card 1, and delivering and receiving required data

if needed. And in step S2, IC card 1 performs service discernment processing of IC card 1 later mentioned using drawing 17 and drawing 19 by communicating with the reader writer 2, and delivering and receiving required data if needed.

[0085] And by communicating with IC card 1, and delivering and receiving required data if needed, when service discernment processing of the reader writer 2 of step S1 and service discernment processing of IC card 1 of step S2 terminate normally, in step S3, the reader writer 2 performs authentication key discernment processing of the reader writer 2 later mentioned using drawing 20 , drawing 22 , and drawing 27 . And in step S4, IC card 1 performs authentication key discernment processing of IC card 1 later mentioned using drawing 21 , drawing 23 , and drawing 28 by communicating with the reader writer 2, and delivering and receiving required data if needed.

[0086] Next, by a user's inputting desired service in the reader writer 2 corresponding to two or more services, and judging it whether activation of the service is possible to be IC card 1 corresponding to two or more services with reference to the flow chart of drawing 16 , explains service discernment processing of the reader writer 2 performed in step S1 of drawing 15 .

[0087] To IC card 1, through the communications department 91, the control section 101 of the reader writer 2 transmits an IC card detection command, and judges whether the ACK signal (signal which IC card 1 transmitted in step S22 of

drawing 17 mentioned later) was received from IC card 1 in step S12 in step S11. In step S12, when it is judged that the ACK signal is not received, processing of step S12 is repeated until it is judged that the ACK signal was received.

[0088] When it is judged in step S12 that the ACK signal was received, it sets to step S13 (namely, when the reader writer 2 is equipped with IC card 1). A control section 101 According to the signal which shows the actuation which the user inputted using the input section 106, the service ID corresponding to giving [which a user wishes] is transmitted to IC card 1 through the communications department 91 based on the service for which it opted beforehand.

[0089] In step S14, a control section 101 receives the signal (signal which IC card 1 transmitted in step S25 or step S26 of drawing 17 mentioned later) transmitted from IC card 1. In step S15, the data which the control section 101 received in step S14 judge whether it is an ACK signal. In step S15, when the received signal is judged not to be an ACK signal (that is, for it to be a NACK signal), in step S16, a control section 101 outputs and displays the data corresponding to an error message on a display 105, and ends processing (that is, processing does not progress to step S3 of drawing 15). In step S15, when the received signal is judged to be an ACK signal, processing progresses to step S3 of drawing 15 .

[0090] Next, with reference to the flow chart of drawing 17 , the service

discernment processing of IC card 1 performed in parallel to service discernment processing of the reader writer 2 explained using drawing 16 is explained in step S2 of drawing 15 . In addition, although here explains as that to which processing is performed in IC card 1 explained using drawing 3 , when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0091] In step S21, in step S11 of drawing 16 , the control section 31 of IC card 1 receives the IC card detection command which the reader writer 2 transmitted through the communications department 21, and transmits an ACK signal to the reader writer 2 in step S22.

[0092] A control section 31 is set to step S13 of drawing 16 in step S23. The service ID which received the service ID which the reader writer 2 transmitted through the communications department 21, and was received in step S24 The module with which IC card 1 corresponds (although it corresponds to the memory 32 of the IC card processing section 22 here since the processing in IC card 1 explained using drawing 3 is explained) In the case of IC card 1 explained using drawing 4, with the method with which the reader writer 2 corresponds For example, the memory 62 of the common key service processing section 52 Or it judges whether the service ID received in whether it is ID registered while corresponding to the memory 62 of the public key service processing section,

and step S23 is registered into SRA46 explained using drawing 6 .

[0093] In step S24, when the received service ID is judged to be registered into a module, in step S25, a control section 31 transmits an ACK signal to the reader writer 2 through the communications department 21, and processing progresses to step S4 of drawing 15 . In step S24, when the received service ID is judged not to be registered into a module, in step S26, a control section 31 transmits a NACK signal to the reader writer 2 through the communications department 21, and processing is ended (that is, it does not progress to step S4 of drawing 15).

[0094] Next, with reference to the flow chart of drawing 18 , it sets to IC card 1 corresponding to two or more services, and the reader writer 2 corresponding to two or more services. By extracting corresponding IC card 1 and the service which can perform the reader writer 2, making it display on the display 105 of the reader writer 2, and making the service for which a user asks choose from those services Service discernment processing of the reader writer 2 performed in step S1 of drawing 15 in the case of performing service discernment is explained.

[0095] The control section 101 of the reader writer 2 judges whether the service ID list which IC card 1 transmitted was received in step S31 in step S52 of drawing 19 which transmits to IC card 1 through the communications department 91, and mentions a service ID list transmitting command later in step S32. In step S32, when it is judged that the service ID list is not received, processing of

step S32 is repeated until it is judged that the service ID list was received.

[0096] In step S32, when it is judged that the service ID list was received, in a control section 101, in step S33, the service ID indicated by the received service ID list judges whether the service which the reader writer 2 supports is included (that is, is the service ID memorized by the memory 103 of the reader writer 2 included or not?).

[0097] In step S33, when it is judged that the service corresponding to a reader writer is included in the received service ID list, in step S34, a control section 101 judges whether the correspondence service included in the service ID list is plurality. In step S34, when correspondence service is judged not to be plurality (that is, for it to be only one), processing progresses to step S37.

[0098] In step S34, when correspondence service is judged to be plurality, in step S35, a control section 101 generates the data for displaying two or more correspondence services on a display 105, is made to output and display them on a display 105, and receives the input of giving [which a user wishes] from the input section 106 in step S36. Or priority information is included in each service and the highest service of a priority may be made to be chosen from from automatically among two or more correspondence services.

[0099] In step S37, when it is judged in step S34 that correspondence service is only one, a control section 101 When correspondence service is judged to be

plurality in step S34, the service ID corresponding to the service In step S36, the service ID corresponding to giving [which the user inputted using the input section 106 / to wish one's service] is transmitted to IC card 1 through the communications department 91, and processing progresses to step S3 of drawing 15 .

[0100] When it is judged that the service corresponding to a reader writer is not included in the received service ID list in step S33, a control section 101 In step S38, through the communications department 91, a NACK signal is transmitted to IC card 1, the same processing as step S16 of drawing 16 is made in step S39, and processing is ended (that is, processing does not progress to step S3 of drawing 15).

[0101] Next, with reference to the flow chart of drawing 19 , the service discernment processing of IC card 1 performed in parallel to service discernment processing of the reader writer 2 explained using drawing 18 is explained in step S2 of drawing 15 . In addition, although here explains as that to which processing is performed in IC card 1 explained using drawing 3 , when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0102] In step S51, the reader writer 2 receives the service ID transmitting command transmitted in step S31 of drawing 18 through the communications

department 21, and the control section 31 of IC card 1 generates the service ID list (namely, list of services ID registered into SRA46 of memory 32) with which he corresponds in step S52, and transmits to the reader writer 2 through the communications department 21.

[0103] A control section 31 receives the data which the reader writer 2 transmitted to IC card 1 in step S37 or step S38 of drawing 18 through the communications department 21 in step S53, and the data received from the reader writer 2 judge whether it is a NACK signal in step S54. In step S54, when the received signal is judged to be a NACK signal, processing is ended (that is, processing does not progress to step S4 of drawing 15). (namely, when the received data are the signal which the reader writer 2 transmitted to IC card 1 in step S38 of drawing 18)

[0104] In step S54, when it is judged that the data received from the reader writer 2 are not a NACK signal, in step S55, a control section 31 judges whether the service ID received from the reader writer 2 is registered into SRA46 of its own memory 32 (namely, when the received data are the service ID which the reader writer 2 transmitted to IC card 1 in step S37 of drawing 18).

[0105] In step S55, when it is judged that Service ID is not registered, processing is ended (that is, processing does not progress to step S4 of drawing 15). In step S55, when it is judged that Service ID is registered, processing progresses

to step S4 of drawing 15 .

[0106] Next, when authentication key discernment is performed with reference to the flow chart of drawing 20 using the key information for authentication that it explained using drawing 7 (A), authentication key discernment processing of the reader writer 2 performed in step S3 of drawing 15 is explained.

[0107] It is the service ID corresponding to the service from which the control section 101 of the reader writer 2 was discriminated in step S61 by service discernment processing of step S1 of drawing 15 , and step S2 (here). Read from memory 103, transmit to IC card 1 through the communications department 91, and the authentication key ID corresponding to one of the authentication keys which belong for making corresponding service ID into ID_S is set to step S62. The data which IC card 1 transmits are received in step S73 or step S75 of drawing 21 mentioned later.

[0108] In step S63, the data which the control section 101 received from IC card 1 in step S62 judge whether it is an ACK signal. When it is judged in step S63 that the ACK signal was received, it sets to step S64. A control section 101 The cipher-processing section 33 is controlled and it sets to step S61. The inside of the public key processing section 111 of the cipher-processing section 102, or the common key processing section 112, By choosing and controlling the processing section which performs authentication processing using the

authentication key corresponding to the authentication key ID transmitted to IC card 1 Processing is ended, after starting mutual recognition processing with IC card 1, and key share processing, sharing IC card 1 and the session key Kses and completing mutual recognition processing.

[0109] In step S63, when it is judged that the ACK signal is not received, in step S65, the same processing as step S16 of drawing 16 is made, and processing is ended (namely, when it is judged that the NACK signal was received).

[0110] Next, with reference to the flow chart of drawing 21 , the authentication key discernment processing of IC card 1 performed in parallel to authentication key discernment processing of the reader writer 2 of drawing 20 is explained in step S4 of drawing 15 . In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0111] The control section 31 of IC card 1 judges whether the authentication key ID which received the authentication key ID which the reader writer 2 transmitted through the communications department 21, and was received in step S71 in step S72 is registered into the field to which the data about ID_S of SRA46 of memory 32 are memorized in step S61 of drawing 20 in step S71.

[0112] When it is judged in step S72 that the authentication key ID is registered,

a control section 31 In step S73, through the communications department 21, transmit an ACK signal to the reader writer 2, and it sets to step S74. By choosing and controlling the direction which performs authentication processing with the authentication key specified as the reader writer 2 among the public key processing section 41 of the cipher-processing section 33, or the common key processing section 42 Mutual recognition processing is performed, the reader writer 2 and the session key Kses are shared, and processing is ended after termination of mutual recognition processing. In step S72, when it is judged that the authentication key ID is not registered, in step S75, a control section 31 transmits a NACK signal to the reader writer 2 through the communications department 21, and processing is ended.

[0113] In the processing explained using drawing 20 and drawing 21 , IC card 1 and the reader writer 2 perform mutual recognition with the authentication key specified by the reader writer 2 corresponding to the service ID of the service identified by processing of step S1 of drawing 15 , and step S2.

[0114] For example, it makes to perform high-speed processing by authentication processing based on a common key into a default, and when the version of a common key is old, based on a public key, it may be made to carry out authentication processing, when two kinds of authentication keys, a common key and a public key, are prepared to a certain service.

[0115] Next, with reference to the flow chart of drawing 22 , authentication key discernment processing of the reader writer 2 in case two kinds of authentication keys, a common key and a public key, are prepared is explained to the service corresponding to the service ID of the service identified by processing of step S1 of drawing 15 and step S2 which are performed in step S3 of drawing 15 .

[0116] The control section 101 of the reader writer 2 transmits the common key version information-requirements command of the authentication key corresponding to the service ID of the service identified by processing of step S1 of drawing 15 , and step S2 to IC card 1 through the communications department 91, and receives the common key version information which IC card 1 transmitted through the communications department 91 in step S92 of drawing 23 mentioned later in step S82 in step S81.

[0117] In step S83, a control section 101 judges whether a common key version is effective based on the common key version information received in step S82. In step S83, when it is judged that a common key version is effective, after a control section 101 transmits a mutual recognition initiation command with a common key to IC card 1, controlling the common key processing section 112 of the cipher-processing section 102, starting mutual recognition with a common key, sharing IC card 1 and the session key Kses and completing mutual recognition, processing is ended in step S84.

[0118] In step S83, when it is judged that a common key version is not effective, after a control section 101 transmits the mutual recognition initiation command by the public key to IC card 1, controlling the public key processing section 111 of the cipher-processing section 102, starting the mutual recognition by the public key, sharing IC card 1 and the session key Kses and completing mutual recognition, processing is ended in step S85.

[0119] Next, with reference to the flow chart of drawing 23 , the authentication key discernment processing of IC card 1 performed in parallel to authentication key discernment processing of the reader writer 2 explained using drawing 22 is explained in step S4 of drawing 15 . In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0120] In step S91, in step S81 of drawing 22 , the control section 31 of IC card 1 receives the common key version information-requirements command which the reader writer 2 transmitted, and transmits common key version information to the reader writer 2 through the communications department 21 in step S92.

[0121] A control section 31 judges whether the mutual recognition initiation command which received the mutual recognition initiation command which the reader writer 2 transmitted, and was received in step S93 in step S94 is a mutual

recognition initiation command with a common key in step S84 or step S85 of drawing 22 in step S93.

[0122] In step S94, when it is judged that it is a mutual recognition initiation command with a common key, after a control section 31 controls the common key processing section 42 of the cipher-processing section 33, starting mutual recognition with a common key, sharing the reader writer 2 and the session key Kses and completing mutual recognition, processing is ended in step S95.

[0123] In step S94, when it is judged that it is not a mutual recognition initiation command with a common key (that is, it is a mutual recognition initiation command by the public key), after a control section 31 controls the public key processing section 41 of the cipher-processing section 33, starting the mutual recognition by the public key, sharing the reader writer 2 and the session key Kses and completing mutual recognition, processing is ended in step S96.

[0124] By processing explained using drawing 22 and drawing 23 , IC card 1 and the reader writer 2 perform mutual recognition using a public key, when it is going to perform mutual recognition with a common key with a quick authentication rate first and mutual recognition with a common key cannot be performed (for example, when the version of a corresponding common key is old etc.).

[0125] Mutual recognition by the public key is performed in processing of step

S85 of drawing 22 , and step S96 of drawing 23 . The certificate of the reader writer 2 shown in drawing 24 (A) is memorized by SRA46 of the memory 103 of the reader writer 2. Moreover, the certificate of IC card 1 shown in drawing 24 (B) is memorized by SRA46 of the memory 32 of IC card 1.

[0126] As shown in drawing 24 (A) and drawing 24 (B), in each certificate The version number of a certificate, the serial number of the certificate which a certificate authority assigns, the algorithm and parameter that were used for the signature, The identifier of a certificate authority, the expiration date of a certificate, the reader writer 2, or the identifier of IC card 1 (ID), By making an irreversible Hash Function (data compression function) which used and explained drawing 5 to the public key Kpsp of the reader writer 2 or the public key Kpu of IC card 1, and the whole message act It consists of digital signatures which created the message digest and were created by enciphering a message digest with the private key Ksca of a certificate authority.

[0127] Next, signature generation processing is explained with reference to the flow chart of drawing 25 . Here, the case where a digital signature is generated is explained using an elliptic curve cryptosystem method (ellipse DSA signature). Here, also in the reader writer 2, although the control section 31 of IC card 1 explains the processing performed by controlling DSA signature generation / verification section 72 of the public key processing section 41, since same

processing is performed, the explanation about processing of the reader writer 2 is omitted.

[0128] In step S101, a control section 31 recognizes a parameter required for signature generation processing. namely, p -- the characteristic, and a and b -- the multiplier of an elliptic curve, and an elliptic curve -- let a message and Ks as a private key and let [y2=x3+ax+b and G / the base point on an elliptic curve, and r] G and KsG be public keys for the order of G, and M.

[0129] In step S102, DSA signature generation / verification section 72 of the public key processing section 41 is the random-number generation section which is not illustrated, it generates u used as 0<u<r, u Doubles a public key G using the random number u generated in step S102 in step S103, and computes V used as V=uG= (Xv, Yv).

[0130] In step S104, DSA signature generation / verification section 72 computes c=Xv mod r, and judges whether it is c= 0 in step S105 based on the count result of S104. In step S105, when it is judged that it is c= 0, as for processing, return and processing after it are repeated by step S102.

[0131] It computes [f=SHA -1 (M) which is / in / when it is judged in step S105 that it is not c= 0 / step S106 / the hash value of Message M, (SHA-1 being used as a Hash Function here), and], it sets to step S107, and DSA signature generation / verification section 72 is d= [(f+cKs) /u]. mod r is calculated.

[0132] In step S108, DSA signature generation / verification section 72 judges whether it is d= 0 based on the count result of step S107. In step S108, when it is judged that it is d= 0, as for processing, return and processing after it are repeated by step S102. In step S108, when it is judged that it is not d= 0, in step S109, DSA signature generation / verification section 72 sets signature data to (c, d), and processing is ended.

[0133] Thus, the reader writer 2 which received the digital signature generated in IC card 1 carries out processing which verifies the digital signature which received. Signature verification processing is explained with reference to the flow chart of drawing 26 . Here, also in IC card 1, although the control section 101 of the reader writer 2 explains the processing performed by controlling DSA signature generation / verification section 72 of the public key processing section 41, since same processing is performed, the explanation about processing of IC card 1 is omitted.

[0134] In step S111, a control section 101 recognizes a parameter required for signature generation processing. namely, p -- the characteristic, and a and b -- the multiplier of an elliptic curve, and an elliptic curve -- let a message and Ks as a private key and let [y2=x3+ax+b and G / the base point on an elliptic curve, and r] G and KsG be public keys for the order of G, and M.

[0135] DSA signature generation / verification section 72 of the public key

processing section 41 judges whether they are 0<c<r and 0<d<r in step S112 based on the value of c and d of the received signature data.

[0136] In step S112, when it is judged that they are not 0<c<r and 0<d<r, processing progresses to step S120. In step S112, when it is judged that they are 0<c<r and 0<d<r, in step S113, DSA signature generation / verification section 72 computes f=SHA -1 (M) which is the hash value of Message M, and calculates h= 1-/d mod r in step S114.

[0137] Using the value of h computed in step S114, in step S115, DSA signature generation / verification section 72 computes h1=fh and h2=ch mod r, and computes P=(Xp, Yp) =h1 G+h2KsG in step S116.

[0138] In step S117, DSA signature generation / verification section 72 judges whether the value of P is an infinite point from the calculation result of step S116. Here, when the value of P is an infinite point, it is possible to judge whether the value of P is an infinite point in step S116 based on the ability not to acquire the solution of h1 G+h2KsG. In step S117, when it is judged that P is an infinite point, processing progresses to step S120.

[0139] In step S117, when the value of P is judged not to be an infinite point, in step S118, DSA signature generation / verification section 72 judges whether c=Xp mod r is realized. In step S118, when it is judged that c=Xp mod r is not realized, processing progresses to step S120.

[0140] In step S118, when it is judged that c=Xp mod r is realized, in step S119, DSA signature generation / verification section 72 judges the received signature to be the right, and processing is ended.

[0141] When it is judged that p is an infinite point in step S117 when it is judged in step S112 that they are not 0<c<r and 0<d<r, or when it is judged in step S118 that c=Xp mod r is not realized, in step S120, it judges that DSA signature generation / verification section 72 of the received signature is not right, and processing is ended.

[0142] Moreover, authentication key discernment is performed using the key information for authentication that it explained using drawing 7 (B). When two or more authentication keys by which the level division was carried out to a certain service are stored, authentication processing is preferentially started from the key of a low, and the version of the key is judged, and when the version of the key is old, it may be made to perform authentication processing using the authentication key of higher level.

[0143] Next, authentication key discernment processing of the reader writer 2 in case two or more authentication keys which are performed in step S3 of drawing 15 and by which the level division was carried out to a certain service are stored with reference to the flow chart of drawing 27 is explained.

[0144] In step S131, through the communications department 91, the control

section 101 of the reader writer 2 transmits a key level negotiation command to IC card 1, and receives key version information V in level N which IC card 1 transmits through the communications department 91 in step S143 of drawing 28 mentioned later in step S132.

[0145] In step S133, a control section 101 judges whether the level N of key version information V which received in step S132 is N> 0. In step S133, when it is judged that it is not N> 0, processing progresses to step S137.

[0146] In step S133, when it is judged that it is N> 0, in step S134, a control section 101 judges whether the key version information in level N is effective based on key version information V which received in step S132.

[0147] In step S134, when it is judged that the key version in level N is not effective, in step S135, a control section 101 transmits a NACK signal to IC card 1 through the communications department 91, and, as for processing, return and processing after it are repeated by step S132 (namely, when it is judged that the version of a key is old).

[0148] In step S134, when it is judged that the key version in level N is effective, in step S136, a control section 101 transmits an ACK signal to IC card 1 through the communications department 91, and processing is ended.

[0149] In step S133, when it is judged that it is not N> 0, in step S137, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0150] Next, with reference to the flow chart of drawing 28 , the authentication key discernment processing of IC card 1 performed in parallel to authentication key discernment processing of the reader writer 2 explained using drawing 27 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0151] In step S141, in step S131 of drawing 27 , the control section 31 of IC card 1 receives the key level negotiation command which the reader writer 2 transmitted, and sets the present key level N to N= 1 in step S142.

[0152] In step S143, a control section 31 transmits key version information V in the present key level N and its level to the reader writer 2 through the communications department 21, and receives the data which the reader writer 2 transmitted in step S135 or step S136 of drawing 27 in step S144.

[0153] In step S145, a control section 31 judges whether the signal received from the reader writer 2 is an ACK signal in step S144. In step S145, when it is judged that the signal received from the reader writer 2 is not an ACK signal, in step S146, a control section 31 considers as N=N +1, and judges whether the value of N is over the predetermined maximum level in step S147.

[0154] In step S147, when it is judged that N is not over the maximum level, as

for processing, return and processing after it are repeated by step S143. In step S147, when it is judged that N is over the maximum level, in step S148, a control section 31 sets current level to N= 0 (N= 0 shall show an exception condition), and, as for processing, return and processing after it are repeated by step S143.

[0155] In step S145, when it is judged that the signal received from the reader writer 2 is an ACK signal, processing is ended.

[0156] Although the processing about IC card 1, service discernment of the reader writer 2, and authentication key discernment was explained using drawing 15 thru/or drawing 28 For example, when equipping with IC card 1 and performing registration of new service, and when deletion of service was performed to the reader writer 2-11 for service registration explained using drawing 2 , as it explained to it using drawing 10 In order to perform authentication processing using the authentication key Kreg for service registration memorized by the memory 103 of the reader writer 2-11 for service registration, it is not necessary to use mutual recognition processing which was explained using drawing 15 thru/or drawing 28 .

[0157] Next, with reference to the flow chart of drawing 29 , service registration processing of the reader writer 2-11 for service registration is explained.

[0158] In step S151, through the communications department 91, the control section 101 of the reader writer 2-11 for service registration transmits a service

registration command to IC card 1, performs IC card 1 and mutual recognition with the key Kreg for service registration in step S152, and shares the session key Kses.

[0159] In step S153, a control section 101 transmits a free-area check command to IC card 1 through the communications department 91, and receives the data transmitted from IC card 1 in step S175 or step S176 of drawing 30 mentioned later in step S154.

[0160] In step S155, a control section 101 judges whether the signal received from IC card 1 is an ACK signal in step S154. When the signal received from IC card 1 is judged to be an ACK signal, in step S155, in step S156, a control section 101 controls the common key processing section 112 of the cipher-processing section 102, makes the registration data newly registered into the memory 32 of IC card 1 encipher with the session key Kses, and transmits encryption data to IC card 1 through the communications department 91 in step S157.

[0161] The notice of the completion of data registration to which IC card 1 transmitted the control section 101 in step S180 of drawing 30 later mentioned in step S158 is received through the communications department 91, the service deletion authorization flag by service authentication is transmitted in step S159, and processing is ended.

[0162] In step S155, when the signal received from IC card 1 is judged not to be an ACK signal, in step S160, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0163] Next, with reference to the flow chart of drawing 30 , the service registration processing of IC card 1 performed in parallel to service registration processing of the reader writer 2-11 for service registration in which it explained using drawing 29 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0164] In step S171, the control section 31 of IC card 1 receives the service registration command which the reader writer 2-11 for service registration transmitted in step S151 of drawing 29 through the communications department 21.

[0165] A control section 31 performs mutual recognition with the key Kreg for service registration, shares the session key Kses with IC card 1, and receives the free-area check command which the reader writer 2-11 for service registration transmitted in step S153 of drawing 29 through the communications department 21 in step S173 in step S172.

[0166] In step S174, a control section 31 judges whether the free area for

registration data is in SRA46 of memory 32. In step S174, when it is judged that there is no free area, in step S175, a control section 31 transmits a NACK signal through the communications department 21 at the reader writer 2-11 for service registration, and processing is ended.

[0167] In step S174, when it is judged that there is a free area, in step S176, a control section 31 transmits an ACK signal to the reader writer 2-11 for service registration through the communications department 21.

[0168] A control section 31 receives the encryption data which the reader writer 2-11 for service registration transmitted through the communications department 21, controls the common key processing section 42 of the cipher-processing section 33 in step S178, and makes the encryption data received in step S177 decode in step S157 of drawing 29 in step S177 using the session key Kses.

[0169] A control section 31 supplies the data decoded with the session key Kses to memory 32, and makes them register into the Service Individual Info field and SRT45 of SRA46 in step S178 in step S179.

[0170] In step S180, through the communications department 21, a control section 31 notifies the completion of registration of data to the reader writer 2-11 for service registration, and sets it to step S181. In step S159 of drawing 29 , the reader writer 2-11 for service registration transmitted. The service deletion authorization flag by service authentication is received, a service deletion

authorization flag is set as the Service Individual Info field of SRA46 of memory 32, and processing is ended.

[0171] Next, with reference to the flow chart of drawing 31 , the service deletion of the reader writer 2-11 for service registration is explained.

[0172] In step S191, the control section 101 of the reader writer 2-11 for service registration receives the input of the service ID corresponding to the service to delete which the user inputted using the input section 106 (here, the service whose corresponding service ID is ID_S shall be deleted).

[0173] In step S192, the same processing as step S152 of drawing 29 is made. A control section 101 judges whether the error message which transmitted ID_S region Delete command to IC card 1, and IC card 1 transmitted to it in step S205 of drawing 32 mentioned later in step S194 was received through the communications department 91 in step S193.

[0174] In step S194, when it is judged that the error message was received, in step S195, the same processing as step S16 of drawing 16 is made, and processing is ended. In step S194, when it is judged that an error message was not received, processing is ended.

[0175] Next, with reference to the flow chart of drawing 32 , the service deletion of IC card 1 performed in parallel to the service deletion of the reader writer 2-11 for service registration explained using drawing 31 is explained. In addition,

although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0176] In step S201, the same processing as step S172 of drawing 30 is performed. The control section 31 of IC card 1 judges whether the justification of ID_S region Delete command which received in step S202 was verified in step S193 of drawing 31 in step S202 by receiving ID_S region Delete command which the reader writer 2-11 for service registration transmitted, and checking whether there are any data corresponding to ID_S region in step S203 etc.

[0177] In step S203, when it is judged that the justification of ID_S region Delete command was verified, in step S204, a control section 31 deletes the field corresponding to ID_S of memory 32 from SRT45 and SRA46, and processing is ended.

[0178] In step S203, when it is judged that the justification of ID_S region Delete command was not verified, in step S205, a control section 31 transmits an error message to the reader writer 2-11 for service registration through the communications department 21, and processing is ended.

[0179] Service deletion explained using drawing 31 and drawing 32 can also be performed with the general reader writer 2-12 and IC card 1. With reference to the flow chart of drawing 33 , the service deletion of the general reader writer

2-12 is explained.

[0180] In step S211, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, in step S212, authentication key discernment processing of the reader writer 2 explained using drawing 20 , drawing 22 , or drawing 27 is performed, and the same processing as step S193 of drawing 31 is performed in step S213.

[0181] In step S214, the control section 101 of the general reader writer 2-12 receives the signal which IC card 1 transmits in step S227 or step S228 of drawing 34 mentioned later. And in step S215 and step S216, the same processing as step S15 of drawing 16 and step S16 is performed, and processing is ended.

[0182] Next, with reference to the flow chart of drawing 34 , the service deletion of IC card 1 performed in parallel to the service deletion of the general reader writer 2-12 explained using drawing 33 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0183] In step S221, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21 , drawing 23 ,

or drawing 28 is performed in step S232.

[0184] In step S223, a control section 31 receives ID_S region Delete command which the general reader writer 2-12 transmitted through the communications department 21 in step S213 of drawing 33 . In step S224, the same processing as step S203 of drawing 32 is performed.

[0185] In step S224, when it is judged that the justification of a command was not verified, processing progresses to step S228. In step S224, when it is judged that the justification of a command was verified, in step S225, a control section 31 judges whether the service deletion authorization flag is set as the Service Individual Info field of SRA46 of memory 32.

[0186] In step S225, when it is judged that the service deletion authorization flag is not set up, processing progresses to step S228. In step S225, when it is judged that the service deletion authorization flag is set up, in step S226, the same processing as step S204 of drawing 32 is made, in step S227, a control section 31 transmits an ACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0187] In step S224, when it is judged that the justification of a command was not verified, or when it is judged in step S225 that the service deletion authorization flag is not set up, in step S228, a control section 31 transmits a NACK signal to the general reader writer 2-12 through the communications

department 21, and processing is ended.

[0188] Next, service acquisition processing of the general reader writer 2-12 performed when a user receives the service registered into IC card 1 by the general reader writer 2-12 with reference to the flow chart of drawing 35 is explained.

[0189] In step S231, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and authentication key discernment processing of the reader writer 2 explained using drawing 20 , drawing 22 , or drawing 27 is performed in step S232.

[0190] In step S233, the control section 101 of the general reader writer 2-12 transmits the data demand command of ID_S region to IC card 1 through the communications department 91.

[0191] A control section 101 receives the data transmitted from IC card 1, controls the common key processing section 112 of the cipher-processing section 102 in step S235, and makes the encryption data received in step S234 decode in step S245 of drawing 36 mentioned later in step S234 using the session key Kses. A control section 101 performs predetermined data processing, such as subtraction of cybermoney, and addition, using the decoded data, and processing is ended.

[0192] Next, with reference to the flow chart of drawing 36 , the service data

acquisition processing of IC card 1 performed in parallel to service data acquisition processing of the general reader writer 2-12 in which it explained using drawing 35 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0193] In step S241, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21 , drawing 23 , or drawing 28 is performed in step S232.

[0194] In step S243, the control section 31 of IC card 1 receives the data demand command of ID_S region which the general reader writer 2-12 transmitted in step S233 of drawing 35 through the communications department 21. In step S244, a control section 31 controls the common key processing section 42 of the cipher-processing section 33, makes the data registered into the field corresponding to ID_S of memory 32 encipher using the session key Kses, and transmits the data enciphered through the communications department 21 to the general reader writer 2-12 in step S245, and processing is ended.

[0195] Moreover, in IC card 1 and the general reader writer 2-12, when the

permission information corresponding to SRT45 explained using drawing 8 when transfer of the information about a certain service was made is recorded, it is possible to deliver and receive information about the service except transfer of the present information being made. With reference to the flow chart of drawing 37 , the service data acquisition processing of the general reader writer 2-12 performed during activation of the service corresponding to the service ID of those other than ID_S is explained.

[0196] In step S251 thru/or step S254, the same processing as step S231 of drawing 35 thru/or step S234 is performed. In step S255, the data which the control section 101 of the general reader writer 2-12 received from IC card 1 in step S254 judge whether it is a NACK signal.

[0197] In step S255, when the received data are judged not to be a NACK signal, in step S256, the same processing as step S235 of drawing 35 is performed, and processing is ended. In step S255, when the received data are judged to be a NACK signal, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0198] Next, with reference to the flow chart of drawing 38 , the service data acquisition processing of IC card 1 performed in parallel to service data acquisition processing of the general reader writer 2-12 in which it explained using drawing 37 is explained. In addition, although IC card 1 explained also

here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4 , same processing is performed fundamentally.

[0199] In step S261 thru/or step S263, the same processing as step S241 of drawing 34 thru/or step S243 is performed. In addition, at step S261, authentication of different service ID_T from service ID_S shall be performed. In step S264, the control section 31 of IC card 1 judges whether ID_S region corresponding to the data demand command received to SRT45 and SRA46 of memory 32 in step S263 is registered. In step S264, when it is judged that ID_S region is not registered, processing progresses to step S269.

[0200] When it is judged in step S264 that ID_S region is registered, a control section 31 In step S265, from the permission information field corresponding to ID_S of SRT45 of memory 32, acquire the permission information on ID_S and it sets to step S266. It judges whether reading of the data of ID_S is permitted at the time of ID_T authentication (). That is, it judges whether read-out authorization of data, i.e., ro, and rw are indicated in the permission information field corresponding to ID_S of SRT45 at the time of authentication by ID_T. In step S266, when it is judged that reading of data is not permitted, processing progresses to step S269.

[0201] In step S266, when it is judged that reading of data is permitted, in step

S267 and step S268, the same processing as step S244 of drawing 36 and step S245 is performed, and processing is ended.

[0202] In step S264, when it is judged that ID_S region is not registered, or when it is judged in step S266 that reading of data is not permitted, in step S269, a control section 31 transmits a NACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0203] After data are acquired from IC card 1 by the general reader writer 2-12 and predetermined processing is made by service data acquisition processing in which it explained using drawing 35 thru/or drawing 48 , the general reader writer 2-12 performs processing which writes in data to the predetermined field of SRT45 of the memory 32 of IC card 1, or SRA46 if needed.

[0204] Next, with reference to the flow chart of drawing 39 , service data write-in processing of the general reader writer 2-12 is explained.

[0205] In step S281, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and authentication key discernment processing of the reader writer 2 explained using drawing 20 , drawing 22 , or drawing 27 is performed in step S282.

[0206] The control section 101 of the general reader writer 2-12 In step S283, in order to write in the memory 32 of IC card 1 Control the common key processing section 112 of the cipher-processing section 102, make it encipher using the

session key Kses, and the data transmitted to IC card 1 are set to step S284. The data enciphered as the data write command in step S284 are transmitted to IC card 1 through the communications department 91, and processing is ended.

[0207] Next, with reference to the flow chart of drawing 40 , the service data write-in processing of IC card 1 performed in parallel to service data write-in processing of the general reader writer 2-12 in which it explained using drawing 39 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0208] In step S291, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21, drawing 23, or drawing 28 is performed in step S232.

[0209] In step S293, a control section 31 receives the data write command and encryption data which the general reader writer 2-12 transmitted in step S284 of drawing 39 through the communications department 21. A control section 31 writes the data which were made to decode the data which controlled the common key processing section 42 of the cipher-processing section 33, and were received using the session key Kses, and decoded them in step S295 in

step S294 in the service storing field corresponding to ID_S of SRT45 and SRA46 of memory 32, and processing is ended.

[0210] Moreover, in IC card 1 and the general reader writer 2-12, when the permission information corresponding to SRT45 explained using drawing 8 when transfer of the information about a certain service was made is recorded, it is possible to perform service data write-in processing about the service except transfer of the present information being made as well as service data acquisition processing in_which it explained using drawing 37 and drawing 38. With reference to the flow chart of drawing 41, the service data write-in processing of the general reader writer 2-12 performed during activation of the service corresponding to the service ID of those other than ID_S is explained.

[0211] In step S301 thru/or step S304, the same processing as step S281 of drawing 39 thru/or step S284 is performed. And in step S305 and step S306, the same processing as step S15 of drawing 16 and step S16 is made, and processing is ended.

[0212] Next, with reference to the flow chart of drawing 42, the service data write-in processing of IC card 1 performed in parallel to service data write-in processing of the general reader writer 2-12 in which it explained using drawing 41 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is

performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0213] In step S311 thru/or step S313, the same processing as step S291 of drawing 40 thru/or step S293 is performed. In addition, at step S311, authentication of different service ID_T from service ID_S shall be performed. In step S314 and step S315, the same processing as step S264 of drawing 38 and step S265 is made, and in step S314, when it is judged that ID_S region is not registered, processing progresses to step S320.

[0214] In step S316, a control section 31 judges whether the writing of data is permitted to service of ID_S at the time of ID_T authentication (that is, it judges whether write-in authorization of the data at the time of ID_T authentication, i.e., rw, is indicated in the permission information field corresponding to ID_S of SRT45). In step S316, when it is judged that the writing of data is not permitted, processing progresses to step S320.

[0215] In step S316, when it is judged that the writing of data is permitted, in step S317 and step S318, the same processing as step S294 of drawing 40 and step S295 is performed. In step S319, a control section 31 transmits an ACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0216] In step S314, when it is judged that ID_S region is not registered, or when

it is judged in step S316 that the writing of data is not permitted, in step S320, a control section 31 transmits a NACK signal to the general reader writer 2-12 through the communications department 21, and processing is ended.

[0217] As explained above, in order to equip the general reader writer 2-12 with IC card 1 and to receive various services in it, authentication processing must be performed using the common key defined for every service, or a public key. These authentication keys are often upgraded for maintenance of security (that is, a key is changed). A user must be made to have to upgrade the authentication key registered into IC card 1 which he has managed to the authentication key of the version near the newest as much as possible by equipping with IC card 1 the reader writer 2-14 for version up explained using drawing 2, or the general reader writer 2-12, and performing key version up processing later mentioned using drawing 43 thru/or drawing 47.

[0218] Next, with reference to drawing 43, key version up processing of the reader writer 2-14 for version up performed using the key for version up (key Kake_vup for version up explained using drawing 6 and drawing 14) defined for every service is explained.

[0219] In step S331, service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and authentication key discernment processing of the reader writer 2 explained using drawing 20,

drawing 22, or drawing 27 is performed in step S332.

[0220] In step S333, the control section 101 of the reader writer 2-14 for version up controls the common key processing section 112 of the cipher-processing section 102, makes the authentication key ID corresponding to the authentication key which upgrades encipher using the session key Kses, and transmits to IC card 1. In step S334, a control section 101 receives the signal which IC card 1 transmits in step S355 or step S360 of drawing 44 mentioned later.

[0221] In step S335, a control section 101 judges whether the signal received from IC card 1 in step S334 is an ACK signal. In step S335, when the received signal is judged not to be an ACK signal, processing progresses to step S339. In step S335, when the received signal is judged to be an ACK signal, in step S336, read the authentication key Kake from memory 103, control the common key processing section 112 of the cipher-processing section 102, it is made to encipher it as the latest version information corresponding to the authentication key which upgrades using the session key Kses, and a control section 101 transmits to IC card 1 through the communications department 91.

[0222] And in step S337, the signal transmitted in step S359 or step S360 of 44 which IC card 1 mentions later is received. In step S338, the same processing as step S335 is made, and in step S338, when the received signal is judged to be

an ACK signal, processing is ended. In step S335 and step S338, when the received signal is judged not to be an ACK signal, in step S339, the same processing as step S16 of drawing 16 is made, and processing is ended.

[0223] Next, with reference to the flow chart of drawing 44, the key version up processing of IC card 1 performed in parallel to key version up processing of the reader writer 2-14 for version up in which it explained using drawing 43 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0224] In step S351, service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and authentication key discernment processing of IC card 1 explained using drawing 21, drawing 23, or drawing 28 is performed in step S352.

[0225] A control section 31 receives the enciphered authentication key ID which the reader writer 2-14 for version up transmitted in step S333 of drawing 43 through the communications department 21, controls the common key processing section 42 of the cipher-processing section 33, and makes the received data decode in step S353 using the session key Kses. In step S354, a control section 31 judges whether the authentication key ID corresponding to

ID_S of SRT45 and SRA46 of memory 32 exists based on the decoded data. In step S354, when it is judged that the authentication key ID does not exist, processing progresses to step S360.

[0226] When it is judged in step S354 that the authentication key ID exists, a control section 31 In step S355, through the communications department 21, transmit an ACK signal to the reader writer 2-14 for version up, and it sets to step S356. In step S336 of drawing 43, the reader writer 2-14 for version up transmitted. The latest version information and the authentication key Kake which were enciphered are received through the communications department 21, the common key processing section 42 of the cipher-processing section 33 is controlled, and the received version information is made to decode using the session key Kses.

[0227] In step S357, the version information received based on the data which the control section 31 decoded judges whether it is the right (that is, is he a version higher than the version information of the already held authentication key or not?). In step S357, when version information is judged not to be right, processing progresses to step S360.

[0228] When judged as the right, in step S357, version information a control section 31 Control the common key processing section 42 of the cipher-processing section 33, make the authentication key Kake decode using

the session key Kses, write in the field to which the authentication key Kake in SRA46 of memory 32 is indicated, and it sets to step S359. An ACK signal is transmitted to the reader writer 2-14 for version up through the communications department 21, and processing is ended.

[0229] In step S354, when it is judged that the authentication key ID does not exist, and when version information is judged not to be right in step S357, in step S360, a control section 31 transmits a NACK signal to the reader writer 2-14 for version up through the communications department 21, and processing is ended.

[0230] Moreover, in IC card 1 and the general reader writer 2-12, when transfer of the information about a certain service is made, it sets. When the permission information corresponding to SRT45 explained using drawing 8 is recorded, It is possible to perform key version up processing about the service except transfer of the present information being made as well as service data acquisition processing in which it explained using drawing 37 and drawing 38, and service data write-in processing in which it explained using drawing 41 and drawing 42. With reference to the flow chart of drawing 45, the key version up processing of the general reader writer 2-12 performed during activation of the service corresponding to the service ID of those other than ID_S is explained.

[0231] In step S371 and step S372, the same processing as step S331 of drawing 44 and step S332 is performed. And the control section 101 of the

general reader writer 2-12 In step S373, transmit to IC card 1 through the communications department 91, and the version up command of the authentication key of the service corresponding to ID_S is set to step S374. In step S397 of drawing 46 mentioned later, or step S405 of drawing 47, the signal which received the data which IC card 1 transmits and was received from IC card 1 in step S375 judges whether it is an ACK signal.

[0232] In step S375, when the received signal is judged not to be an ACK signal, processing progresses to step S382. In step S375, when the received signal is judged to be an ACK signal, in step S376 thru/or step S382, the same processing as step S333 of drawing 43 thru/or step S339 is made, and processing is ended.

[0233] Next, with reference to the flow chart of drawing 46 and drawing 47, the key version up processing of IC card 1 performed in parallel to key version up processing of the reader writer 2-14 for version up in which it explained using drawing 45 is explained. In addition, although IC card 1 explained also here using drawing 3 explains the case where processing is performed, when processing is performed with IC card 1 explained using drawing 4, same processing is performed fundamentally.

[0234] In step S391 and step S392, the same processing as step S351 of drawing 44 and step S352 is performed. In addition, at step S391, authentication

of different service ID_T from service ID_S shall be performed. In step S393, a control section 31 receives the version up command of the authentication key of ID_S which the reader writer 2-14 for version up transmitted in step S373 of drawing 45.

[0235] In step S394 and step S395, the same processing as step S264 of drawing 38 and step S265 is made, and in step S394, when it is judged that ID_S region is not registered, processing progresses to step S405.

[0236] In step S396, a control section 31 judges whether version up of the authentication key of ID_S is permitted at the time of ID_T authentication (that is, it judges whether authorization of vup at the time of ID_T authentication is indicated in the permission information field corresponding to ID_S of SRT45). In step S396, when it is judged that version up of an authentication key is not permitted, processing progresses to step S405.

[0237] In step S396, when it is judged that version up of an authentication key is permitted, in step S397, a control section 31 transmits an ACK signal to the reader writer 2-14 for version up through the communications department 21.

[0238] And in step S398 thru/or step S405, the same processing as step S353 of drawing 44 thru/or step S360 is performed, and processing is ended.

[0239] Next, with reference to the flow chart of drawing 48 thru/or drawing 51, the intermodule communication explained using drawing 13 is explained.

Intermodule communication is performed by IC card 1 explained using drawing 4, and the reader writer 2-13 for intermodule communications. Here, it considers as the common key module 122 which explained the communications department 51 of IC card 1 explained using drawing 4, and the common key service processing section 52 using drawing 13, and explains as a public key module 121 which explained the communications department 53 which explained using drawing 4, and the public key service processing section 54 using drawing 13.

[0240] First, the intermodule communication in the case of differing the session key which the common key module 122 shares with the reader writer 2-13 for intermodule communications, and the session key which the public key module 121 shares with the reader writer 2-13 for intermodule communications with reference to the flow chart of drawing 48 is explained.

[0241] In step S411, the reader writer 2-13 for intermodule communications performs service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18, and in step S412, the public key module 121 of IC card 1 performs service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19, and it shares the session key Kses1 with the inter module reader writer 2-13 between the public key modules 121.

[0242] In step S413 the reader writer 2-13 for intermodule communications Service discernment processing of the reader writer 2 explained using drawing

16 or drawing 18 is performed, and it sets to step S414. The common key module 122 of IC card 1 Service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and the session key Kses2 is shared with the inter module reader writer 2-13 between the common key modules 122.

[0243] In step S415, the control section 101 of the reader writer 2-13 for intermodule communications judges whether two cards, the public key module 121 and the common key module 122, ID were in agreement based on the card ID of IC card 1 obtained in service discernment processing of the reader writer 2 performed in step S411 and step S413. In step S415, when it is judged that Card ID is not in agreement, in step S416, the same processing as step S16 of drawing 16 is performed.

[0244] In step S415, when it is judged that two cards ID are in agreement, in step S417, the control section 101 of the reader writer 2-13 for intermodule communications transmits a module data migration command to the public key module 121.

[0245] In step S418, the control section 61 of the public key module 121 receives a module data migration initiation command from the reader writer 2-13 for intermodule communications, controls the common key processing section 42 of the cipher-processing section 33, makes the data which move encipher with the

session key Kses1, is step S419 and transmits encryption data to the reader writer 2-13 for intermodule communications.

[0246] In step S420, the control section 101 of the reader writer 2-13 for intermodule communications decodes the data which controlled the common key processing section 112 of the cipher-processing section 102, and were received with the session key Kses1, makes data encipher with the session key Kses2 in step S421, and transmits to the common key module 122. In step S422, the control section 61 of the common key module 122 makes the data which controlled the common key processing section 42 of the cipher-processing section 63, and were received decode with the session key Kses2, and the data decoded in step S423 are saved to the field to which memory 62 corresponds, and it uses them.

[0247] Next, with reference to the flow chart of drawing 49, intermodule communication when the session key which the common key module 122 shares with the reader writer 2-13 for intermodule communications, and the session key which the public key module 121 shares with the reader writer 2-13 for intermodule communications are the same is explained.

[0248] In step S431, the reader writer 2-13 for intermodule communications performs service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18, and in step S432, the public key module 121 of IC

card 1 performs service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19, and it shares the session key Kses1 with the inter module reader writer 2-13 between the public key modules 121.

[0249] In step S433 the reader writer 2-13 for intermodule communications Service discernment processing of the reader writer 2 explained using drawing 16 or drawing 18 is performed, and it sets to step S434. The common key module 122 of IC card 1 Service discernment processing of IC card 1 in which it explained using drawing 17 or drawing 19 is performed, and the session key Kses1 is shared with the inter module reader writer 2-13 between the common key modules 122.

[0250] In step S435 thru/or step S439, the same processing as step S415 of drawing 48 thru/or step S419 is performed. And in step S440, the control section 101 of the reader writer 2-13 for intermodule communications transmits the received data to the common key module 122. After enciphering the decoded data with the session key Kses2, it transmitted to the common key module 122, but since the common key module 122 also has the session key Kses1, these processings become unnecessary [decode the received data with the session key Kses1, and / the module] in step S420 and step S421 of drawing 48, here.

[0251] In step S411, the control section 61 of the common key module 122 decodes the data which controlled the cipher-processing section 63 and were

received with the session key Kses1, and the data decoded in step S422 are saved to the field to which memory 62 corresponds, and it uses them.

[0252] Next, although the session key which the common key module 122 shares with the reader writer 2-13 for intermodule communications differs from the session key which the public key module 121 shares with the reader writer 2-13 for intermodule communications with reference to the flow chart of drawing 50 The reader writer 2-13 for intermodule communications the session key which the common key module 122 has It enciphers with another [which the public key module 121 has] session key, and the intermodule communication in the case of being made as [supply / the public key module 121] is explained.

[0253] In step S451 thru/or step S456, the same processing as step S411 of drawing 48 thru/or step S416 is performed. That is, the session key Kses1 is shared with the inter module reader writer 2-13 between the public key modules 121, and the session key Kses2 is shared with the inter module reader writer 2-13 between the common key modules 122.

[0254] In step S457, the control section 101 of the reader writer 2-13 for intermodule communications controls the cipher-processing section 102, makes the session key Kses2 encipher with the session key Kses1, and transmits to the public key module 121. The control section 61 of the public key module 121 takes out the session key Kses2 by making the data which controlled the

common key processing section 42 of the cipher-processing section 33, and were received decode with the session key Kses1.

[0255] In step S459, the same processing as step S417 of drawing 48 is performed. In step S460, the control section 61 of the public key module 121 enciphers the data which move with the session key Kses2, and transmits encryption data to the reader writer 2-13 for intermodule communications.

[0256] In step S461, the same processing as step S440 of drawing 49 is performed. And in step S462 and step S463, the same processing as steps S422 and S423 of drawing 48 is performed.

[0257] Namely, in step S420 and step S421 of drawing 48, decode the received data with the session key Kses1, and although it transmitted to the common key module 122 after enciphering the decoded data with the session key Kses2 Here, like the processing explained using drawing 49, since the common key module 122 and the public key module 121 can obtain the same session key Kses2, it is not necessary to perform these processings.

[0258] And with reference to the flow chart of drawing 51, the public key module 121 and the common key module 122 share common private key K_common, and perform mutual recognition using it, and the intermodule communication in the case of sharing the still more common session key Kses is explained.

[0259] In step S471 and step S472, by common private key K_common, the

public key module 121 and the common key module 122 perform mutual recognition, and share the session key Kses. In step S473, the reader writer 2-13 for intermodule communications offers only the channel of the mutual recognition in step S471 and step S472 (namely, as for sharing of a session key, the public key module 121 and the common key module 122 are not performed).

[0260] In step S474, the same processing as step S417 of drawing 48 is performed. In step S475, the control section 61 of the public key module 121 makes the data which control the common key processing section 42 of the cipher-processing section 33, and move encipher with the session key Kses, and transmits encryption data to the reader writer 2-13 for intermodule communications. And in step S476 thru/or step S478, the same processing as step S421 of drawing 49 thru/or step S423 is performed.

[0261] Namely, in the intermodule communication explained using drawing 51, the reader writer 2-13 for intermodule communications does not encipher the data by which it is only offering the channel of data and intermodule communication is carried out, or does not decode them.

[0262] A series of processings mentioned above can also be performed with software. The software is that the program which constitutes the software installs the computer built into the hardware of dedication, or various kinds of programs, and is installed in a general-purpose personal computer etc. from a record

medium possible [performing various kinds of functions].

[0263] This record medium is constituted apart from a computer by the package media which are distributed in order to provide a user with a program and which consist of the magnetic disk 115 (a floppy (trademark) disk is included) with which the program is recorded, an optical disk 116 (CD-ROM (Compact Disk-Read Only Memory) and DVD (Digital Versatile Disk) are included), a magneto-optic disk 117 (MD (Mini-Disk) is included), or semiconductor memory 118, as shown in drawing 9.

[0264] Moreover, in this specification, even if the processing serially performed in accordance with the sequence that the step which describes the program recorded on a record medium was indicated is not of course necessarily processed serially, it is a juxtaposition thing also including the processing performed according to an individual.

[0265]

[Effect of the Invention] According to the data storage of this invention, a data store method, and the program currently recorded on the record medium The 1st service ID corresponding to [control I/O of the data to an information processor, control the data storage corresponding to two or more services, and] the 1st service of two or more services I/O of data is permitted when I/O of the data about the 1st service is controlled by processing of an input/output control step.

Since storage of the 2nd service ID corresponding to the 2nd service of two or more services was controlled It can make it possible to perform in parallel transfer of the data about other services permitted beforehand, securing security, when transfer of the data about predetermined service is being performed.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing for explaining the communication mode and authentication method of an IC card and a reader writer.

[Drawing 2] It is drawing for explaining the relation of a card publisher, a service provider, and a card holder.

[Drawing 3] It is the block diagram showing the configuration of an IC card.

[Drawing 4] It is the block diagram showing the configuration of an IC card.

[Drawing 5] It is drawing for explaining drawing 3 and the cipher-processing section of drawing 4 .

[Drawing 6] It is drawing for explaining SRA of drawing 3 and drawing 4 .

[Drawing 7] It is drawing for explaining the key information for authentication stored in SRA of drawing 6 .

[Drawing 8] It is drawing for explaining SRT of drawing 3 and drawing 4 .

[Drawing 9] It is the block diagram showing the configuration of a reader writer.

[Drawing 10] It is drawing for explaining the memory information on the reader writer for service registration.

[Drawing 11] It is drawing for explaining the memory information on a general reader writer.

[Drawing 12] It is drawing for explaining the memory information on the reader writer for intermodule communications.

[Drawing 13] It is drawing for explaining intermodule communication.

[Drawing 14] It is drawing for explaining the memory information on the reader writer for version up.

[Drawing 15] It is a flow chart for explaining authentication processing of an IC card and a reader writer.

[Drawing 16] It is a flow chart for explaining service discernment processing of a reader writer.

[Drawing 17] It is a flow chart for explaining service discernment processing of an IC card.

[Drawing 18] It is a flow chart for explaining service discernment processing of a reader writer.

[Drawing 19] It is a flow chart for explaining service discernment processing of

an IC card.

[Drawing 20] It is a flow chart for explaining authentication key discernment processing of a reader writer.

[Drawing 21] It is a flow chart for explaining authentication key discernment processing of an IC card.

[Drawing 22] It is a flow chart for explaining authentication key discernment processing of a reader writer.

[Drawing 23] It is a flow chart for explaining authentication key discernment processing of an IC card.

[Drawing 24] It is drawing for explaining a certificate.

[Drawing 25] It is a flow chart for explaining signature generation processing.

[Drawing 26] It is a flow chart for explaining signature verification processing.

[Drawing 27] It is a flow chart for explaining authentication key discernment processing of a reader writer.

[Drawing 28] It is a flow chart for explaining authentication key discernment processing of an IC card.

[Drawing 29] It is a flow chart for explaining service registration processing of the reader writer for service registration.

[Drawing 30] It is a flow chart for explaining service registration processing of an IC card.

[Drawing 31] It is a flow chart for explaining the service deletion of the reader writer for service registration.

[Drawing 32] It is a flow chart for explaining the service deletion of an IC card.

[Drawing 33] It is a flow chart for explaining the service deletion of a general reader writer.

[Drawing 34] It is a flow chart for explaining the service deletion of an IC card.

[Drawing 35] It is a flow chart for explaining service data acquisition processing of a general reader writer.

[Drawing 36] It is a flow chart for explaining service data transmitting processing of an IC card.

[Drawing 37] It is a flow chart for explaining service data acquisition processing of a general reader writer.

[Drawing 38] It is a flow chart for explaining service data transmitting processing of an IC card.

[Drawing 39] It is a flow chart for explaining service data write-in processing of a general reader writer.

[Drawing 40] It is a flow chart for explaining service data write-in processing of an IC card.

[Drawing 41] It is a flow chart for explaining service data write-in processing of a general reader writer.

[Drawing 42] It is a flow chart for explaining service data write-in processing of an IC card.

[Drawing 43] It is a flow chart for explaining key version up processing of the reader writer for version up.

[Drawing 44] It is a flow chart for explaining key version up processing of an IC card.

[Drawing 45] It is a flow chart for explaining key version up processing of a general reader writer.

[Drawing 46] It is a flow chart for explaining key version up processing of an IC card.

[Drawing 47] It is a flow chart for explaining key version up processing of an IC card.

[Drawing 48] It is a flow chart for explaining intermodule communication processing.

[Drawing 49] It is a flow chart for explaining intermodule communication processing.

[Drawing 50] It is a flow chart for explaining intermodule communication processing.

[Drawing 51] It is a flow chart for explaining intermodule communication processing.

[Description of Notations]

1 IC Card 1 Reader Writer 21 Communications Department 31 Control Section, 32 memory 33 Cipher-processing section 41 Public key processing section, 42 Common key processing section 43 The other cipher-processing sections 45 SRT, 46 SRA 51 Communications department 52 Common key service processing section, 53 Communications department 54 Public key service processing section 61 Control section, 62 Memory, 63 Cipher-processing section 91 Communications department 101 Control section, 102 Cipher-processing section 103 Memory, the 111 public-key processing section 112 Common key processing section 113 The other cipher-processing sections 105 Display 106 Input section 121 Public key module 122 Common key module

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－357365
（P2001－357365A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｒ	５Ｂ０３５
			Ｔ	５Ｂ０５８
19/07		Ｇ０９Ｃ　1/00	６６０Ａ	５Ｊ１０４
19/00		Ｇ０６Ｋ　19/00	Ｈ	
Ｇ０９Ｃ　1/00	６６０		Ｕ	

審査請求　未請求　請求項の数５　ＯＬ　（全 39 頁）

(21)出願番号　特願2000－180051(P2000－180051)

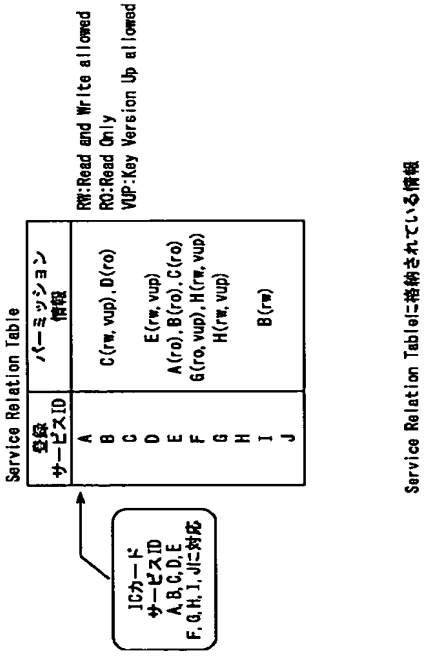
(22)出願日　平成12年６月15日(2000.6.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　白井　太三
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　データ記憶装置およびデータ記憶方法、並びに記録媒体

(57)【要約】
【課題】　１枚のＩＣカードで、セキュリティを確保しつつ、複数のサービスの供給を同時に受けることができるようにする。
【解決手段】　Service Relation Tableには、ＩＤカードに複数のサービスが登録されている場合に、あるサービスを行いながら別のサービスのサービスデータに対してアクセスを許可するためのデータが登録されており、ＩＣカードに登録されているサービスＩＤが記載されている登録サービスＩＤフィールドと、それぞれのサービスＩＤに対応するパーミッション情報が記載されているパーミッション情報フィールドで構成されている。パーミッション情報は、対応するサービスが実行されている場合にアクセスすることができるサービスＩＤと、アクセス可能なサービスＩＤに対して、実行可能な処理を示す情報が記載されている。



1

【特許請求の範囲】

【請求項１】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置において、

前記情報処理装置に対する、前記データの入出力を制御する入出力制御手段と、

複数のサービスに対応するデータの記憶を制御する第１の記憶制御手段と、

前記複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、前記入出力制御手段により前記第１のサービスに関する前記データの入出力が制御されている場合に前記データの入出力が許可される、前記複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御する第２の記憶制御手段とを備えることを特徴とするデータ記憶装置。

【請求項２】　前記第２の記憶制御手段は、前記第２のサービスに関するアクセス権の制限に関する情報の記憶をさらに制御することを特徴とする請求項１に記載のデータ記憶装置。

【請求項３】　前記第２の記憶制御手段は、

前記第２のサービスＩＤが、前記第１のサービスＩＤに対して複数存在する場合、複数の前記第２のサービスＩＤの記憶を制御し、

前記第２のサービスＩＤが、前記第１のサービスＩＤに対して１つも存在しない場合、前記第２のサービスＩＤが空欄となるように記憶を制御することを特徴とする請求項１に記載のデータ記憶装置。

【請求項４】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置のデータ記憶方法において、

前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、

複数のサービスに対応するデータの記憶を制御する第１の記憶制御ステップと、

前記複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、前記入出力制御ステップの処理により前記第１のサービスに関する前記データの入出力が制御されている場合に前記データの入出力が許可される、前記複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御する第２の記憶制御ステップとを含むことを特徴とするデータ記憶方法。

【請求項５】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置用のプログラムであって、

前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、

複数のサービスに対応するデータの記憶を制御する第１の記憶制御ステップと、

前記複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、前記入出力制御ステップの処理により前記第１のサービスに関する前記データの入出力

2

が制御されている場合に前記データの入出力が許可される、前記複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御する第２の記憶制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ記憶装置およびデータ記憶方法に関し、例えば、ＩＣカードと、リーダライタとが、所定のサービスに関するデータの授受を実行している場合において、セキュリティを確保しつつ、予め許可された他のサービスに関するデータの授受を、並行して行うことを可能とするデータ記憶装置およびデータ記憶方法に関する。

【０００２】

【従来の技術】電子マネーシステムや、セキュリティシステムにおいて、ＩＣ（Integrated circuit）カードの利用が増加している。ＩＣカードは、各種処理を行うＣＰＵ（Central Processing Unit）や、処理に必要なデータなどを記憶するメモリを内蔵しており、所定のリーダライタに電気的に接触させた状態で、または電磁波を利用して非接触で、データの送受信が行われる。なお、リーダライタとの間で、電磁波を利用して非接触でデータの送受信を行うＩＣカードには、一般に、その電磁波により、必要な電力が供給される。

【０００３】ＩＣカードと、リーダライタの認証には、共通鍵方式もしくは公開鍵方式が用いられる。共通鍵方式では、暗号化に使用する鍵と、復号に使用する鍵が同じである。共通鍵暗号を使うには、前もって送信者と受信者の間で共通鍵を共有する必要があるため、暗号化に使用した鍵を、通信路とは別の安全な手段を使って、通信相手に届けておく必要がある（すなわち、ＩＣカードとリーダライタが共通鍵を予め共有していなければならない）。暗号化は、基本的には、文字の順序を入れ換える「転置（転字）」と、一定の規則に従ってある文字を別の文字に置き換える「換字」を組み合わせて行われる。どのような順序で入れ換えるか、どの文字とどの文字が置き換えてあるかを示すのが暗号アルゴリズムと鍵である。暗号化において、文字をずらすための換字暗号や文字の順序を変えるための転置暗号が基本的な暗号変換であり、ずらされる文字数などが鍵となる。

【０００４】公開鍵方式は、暗号システムにおいて、「暗号化鍵」と「復号鍵」という２つの鍵をペアで使い、そのうちの暗号化鍵は公開し、復号鍵は、鍵の発行者が管理して秘密にしておくものである。データを送信する場合は、暗号化鍵を使って通信文を暗号化し、受信した側では復号鍵を使って元に戻す。２つの鍵はある数学的な関係に基づいて決められているので、暗号化鍵から復号鍵を求めるのは不可能ではないが、計算量の点から現実的ではない。

【０００５】公開鍵暗号システムは、従来の共通鍵暗号システムに比べて、暗号化鍵は秘匿する必要がないので、暗号化鍵の配布が容易であり、暗号文を復号するには、各ユーザが個々に持っている復号鍵さえあればよいので、復号鍵を配布する必要がなく、更に、デジタル署名によるメッセージの認証機能を持つ、という利点を有するが、共通鍵暗号システムに比べて、認証処理にかかる時間が長くなる。

【０００６】デジタル署名とは、電子メールやオンライン取り引きなどにおいて、そのメッセージが正当な発信者から発信され、途中で改ざんなどが行なわれていないことを示すための方法である。通常の暗号文通信では、公開鍵で暗号化を行うが、例えば、ＲＳＡ（Rivest, Shamir, Adleman）公開鍵暗号システムの場合には、逆に、「復号鍵（秘密鍵）で暗号化を行う」とデジタル署名となる。また、他の暗号方式では、署名を付加したいデータに対して、ハッシュ値を取り、それを秘密鍵で暗号化している。

【０００７】この署名を検証するには、公開鍵が用いられる（すなわち、暗号化鍵と復号鍵の役割が入れ換えられる）。公開鍵は広く公開されているので、だれでもその署名の正当性を簡単に検査することができる。もし公開鍵で暗号文を正しく復元することができ、意味のある文が得られれば、それは正しい発信者であると確認することができる。なぜなら、秘密鍵（署名を行った鍵）を知っているのは正規の発信者だけであり、公開鍵で復元できるようなデジタル署名を作成するには、そのペアとなる秘密鍵を知らなければいけないからである。また、データが改ざんされた場合、データは正しく復号することができなくなるため、改ざんの防止・検出にも利用することができる。署名の検証は、公開鍵を用いて復号した値と、別途、データから計算しなおしたハッシュ値とを比較することにより実行され、一致していれば、データは改ざんされていないと判断され、一致していなければ、データの改ざんが行われたと判断される。

【０００８】また、データの発行元が信頼のおける組織であることを証明するための証明書を発行することを目的とした第３者の組織を、認証局（ＣＡ（Certificate Authority））という。

【０００９】

【発明が解決しようとする課題】従来、ＩＣカードを用いて複数のサービスを受ける場合、１つのサービスを受けている間は、他のサービスを受けることができない。なぜならば、ＩＣカードとリーダライタにおいて、所定のデータを授受するためには、それぞれのデータに対するセキュリティを確保するために、認証処理を行う必要があるからである。しかしながら、例えば、同一のＩＣカードと同一のリーダライタを用いて、プリペイドサービスと電子マネーサービスを受けることができるような場合、プリペイドサービスに関する清算処理を行いながら、電子マネーの充填を行いたいという要求がある。

【００１０】本発明はこのような状況に鑑みてなされたものであり、所定のサービスに関するデータの授受を実行している場合において、セキュリティを確保しつつ、予め許可された他のサービスに関するデータの授受を、並行して行うことを可能とするものである。

【００１１】

【課題を解決するための手段】本発明のデータ記憶装置は、情報処理装置に対する、データの入出力を制御する入出力制御手段と、複数のサービスに対応するデータの記憶を制御する第１の記憶制御手段と、複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、入出力制御手段により第１のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御する第２の記憶制御手段とを備えることを特徴とする。

【００１２】第２の記憶制御手段には、第２のサービスに関するアクセス権の制限に関する情報の記憶を制御させることができる。

【００１３】第２の記憶制御手段には、第２のサービスＩＤが、第１のサービスＩＤに対して複数存在する場合、複数の第２のサービスＩＤの記憶を制御させ、第２のサービスＩＤが、第１のサービスＩＤに対して１つも存在しない場合、第２のサービスＩＤが空欄となるように記憶を制御させることができる。

【００１４】本発明のデータ記憶方法は、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、複数のサービスに対応するデータの記憶を制御する第１の記憶制御ステップと、複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、入出力制御ステップの処理により第１のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御する第２の記憶制御ステップとを含むことを特徴とする。

【００１５】本発明の記録媒体に記録されているプログラムは、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、複数のサービスに対応するデータの記憶を制御する第１の記憶制御ステップと、複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、入出力制御ステップの処理により第１のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御する第２の記憶制御ステップとを含むことを特徴とする。

【００１６】本発明のデータ記憶装置、データ記憶方法および記録媒体に記録されているプログラムにおいては、情報処理装置に対するデータの入出力が制御され、

複数のサービスに対応するデータの記憶が制御され、複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、入出力制御ステップの処理により第１のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶が制御される。

【００１７】

【発明の実施の形態】以下、図を参照して、本発明の実施の形態について説明する。

【００１８】図１に、ＩＣカードとリーダライタの関係を示す。ＩＣカード１は、共通鍵方式による認証と、公開鍵方式による認証の両方の認証サービスに対応することが可能である（それぞれの認証方法については後述する）。非接触式共通鍵対応リーダライタ２－１は、ＩＣカード１と非接触で通信を行い、共通鍵方式で認証を行う。非接触式公開鍵対応リーダライタ２－２は、ＩＣカード１と非接触で通信を行い、公開鍵方式で認証を行う。接触式公開鍵対応リーダライタ２－３は、接触して通信を行い、公開鍵方式で通信を行う。

【００１９】例えば、ＩＣカード１に定期券や運賃の支払いを行うことができるプリペイドカードなどのサービスを提供する情報が含まれており、ＩＣカード１を用いて駅の改札を利用する場合や、ＩＣカード１に、ＩＤカードとしての機能が含まれており、ＩＣカード１を用いて入室許可の認証を行う場合などの、短い処理時間が求められる処理においては、非接触式共通鍵対応リーダライタ２－１を用いて、共通鍵による非接触の通信が行われる。

【００２０】例えば、ＩＣカード１に、電子マネーのサービスを提供する情報が含まれており、店舗などでユーザが購買した商品の清算の処理を行う場合などは、公開鍵方式により認証が行われ、認証処理に時間がかかる。このため、処理時間を特に気にしないような場合は、非接触式公開鍵対応リーダライタ２－２を用いて、非接触で通信を行ってもよいし、処理時間を短縮するために、接触式公開鍵対応リーダライタ２－３を用いて、接触して通信を行うようにしてもよい。

【００２１】図１においては、非接触式共通鍵対応リーダライタ２－１乃至接触式公開鍵対応リーダライタ２－３を、個別のリーダライタとして説明しているが、必要に応じて、１つのリーダライタで、複数の通信方法や複数の認証方法を用いることができるようにしてもよい。

【００２２】次に、図２を用いて、カード発行者、サービス提供者、およびカード保持者について説明する。

【００２３】カード発行者１１は、サービス提供者１２に、ＩＣカード１を保有するカード保持者１３に対して、ＩＣカード１を用いたサービスの提供を行うことを認可し、ＩＣカード１の発行を希望したカード保持者１３に対して、ＩＣカード１を発行する。

【００２４】カード発行者１１から、サービスの認可を受けたサービス提供者１２は、カード発行者１１が有するサービス登録用リーダライタ２－１１に、自分自身がカード保持者１３に提供するサービスに対応するデータ（図６を用いて後述するService Individual Info）を登録する。この登録については、例えば、サービス提供者１２が有する図示しないパーソナルコンピュータなどから、インターネットなどを介して、サービス登録用リーダライタ２－１１に登録するようにしてもよいし、オペレータが手動で登録するようにしてもよい。

【００２５】カード保持者１３は、サービス登録用リーダライタ２－１１を用いて、カード発行者１１から発行されたＩＣカード１に、希望するサービスを登録させることができる。サービス登録用リーダライタ２－１１と、ＩＣカード１のサービス登録処理については、図２９および図３０を用いて後述する。

【００２６】そして、カード保持者１３は、自分自身のＩＣカード１に登録されているサービスの削除を行いたい場合、カード発行者１１が管理するサービス登録用リーダライタ２－１１、もしくは、サービス提供者１２が管理する一般リーダライタ２－１２を用いて、自分自身のＩＣカード１から、サービスを削除させることができる。ＩＣカード１とサービス登録用リーダライタ２－１１のサービス削除処理については、図３１および図３２、ＩＣカード１と一般リーダライタ２－１２のサービス削除処理については、図３３および図３４を用いて後述する。

【００２７】また、カード保持者１３は、例えば、ＩＣカード１に、電子マネーサービスとプリペイドサービスが登録されており、それぞれの価値情報が、ＩＣカード１のそれぞれのサービスに関する情報に記録されている状況で、電子マネーの価値の一部を、プリペイドの価値へ置き換えたい場合、サービス提供者１２が管理するモジュール間通信用リーダライタ２－１３を用いて、自分自身のＩＣカード１の、図１３を用いて後述する公開鍵モジュールと共通鍵モジュールの間で、モジュール間通信を実行させることができる。モジュール間通信用リーダライタ２－１３は、共通鍵方式と、公開鍵方式の２方式に対応するようになされている。ＩＣカード１とモジュール間通信用リーダライタ２－１３との処理については、図４８乃至図５１を用いて後述する。

【００２８】更に、カード保持者１３は、失効してしまった認証鍵の更新（バージョンアップ）を行いたい場合、サービス提供者１２が管理する一般リーダライタ２－１２、もしくは、バージョンアップ用リーダライタ２－１４を用いて、自分自身のＩＣカード１に登録されている認証鍵のバージョンアップを行わせることができる。ＩＣカード１とバージョンアップ用リーダライタ２－１４との鍵バージョンアップ処理については、図４３および４４を用いて、ＩＣカード１と一般リーダライタ

２－１２との鍵バージョンアップ処理については、図４５乃至４７を用いて後述する。

【００２９】図３は、ＩＣカード１の構成を示すブロック図である。

【００３０】ＩＣカード１は、リーダライタ２（リーダライタ２－１乃至２－３、もしくはリーダライタ２－１１乃至２－１４を特に区別する必要のない場合については、これらを総称して、リーダライタ２と称するものとする）との通信を行う通信部２１と、データ処理を実行するＩＣカード処理部２２から構成されている。

【００３１】通信部２１は、対応するＩＣカード１が、図１を用いて説明した非接触式共通鍵対応リーダライタ２－１、もしくは非接触式公開鍵対応リーダライタ２－２である場合、非接触式共通鍵対応リーダライタ２－１、もしくは非接触式公開鍵対応リーダライタ２－２と、電磁波を用いて通信するためのコイルを備えている。また、通信部２１は、ＩＣカード１が、図１を用いて説明した非接触式共通鍵対応リーダライタ２－１、および非接触式公開鍵対応リーダライタ２－２のみならず、接触式公開鍵対応リーダライタ２－３との通信にも対応している場合、非接触式共通鍵対応リーダライタ２－１、もしくは非接触式公開鍵対応リーダライタ２－２と、電磁波を用いて通信するためのコイルと、接触式公開鍵対応リーダライタ２－３と通信するための接触端子を備えている。

【００３２】通信部２１は、リーダライタ２から送信されたデータを受信し、受信したデータが、例えば、ＡＳＫ（Amplitude Shift Keying）やＢＰＳＫ（Binary Phase Shift Keying）を用いて変調されている場合、所定の処理により、受信したデータを復調し、ＩＣカード処理部２２の制御部３１に供給するとともに、ＩＣカード処理部２２の処理により生成されたデータを、制御部３１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、リーダライタ２に送信する。

【００３３】ＩＣカード処理部２２は、制御部３１、メモリ３２、および暗号処理部３３より構成されている。制御部３１は、通信部２１から供給されたデータに従って、暗号処理部３３を制御し、リーダライタ２との認証処理等に必要な暗号処理を実行させたり、必要に応じて、メモリ３２に記録されているデータを読み込んで、通信部２１を介して、リーダライタ２に送信する。

【００３４】メモリ３２は、カードＩＤ、サービス登録用の認証鍵Kreg、認証局の公開鍵であるCA_Pubが記録されているメモリ領域４４、図８を用いて後述するService Relation Table（ＳＲＴ）４５、および図６を用いて後述するService Registration Area（ＳＲＡ）４６で構成されている。

【００３５】暗号処理部３３は、公開鍵処理部４１、共通鍵処理部４２、その他の暗号処理部４３で構成されている。公開鍵処理部４１乃至その他の暗号処理部４３が実行する処理に関する詳細は、図５を用いて後述する。

【００３６】次に、図４は、ＩＣカード１の、図３と異なる構成を示すブロック図である。なお、図４のＩＣカード１においては、図３における場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する（以下、同様）。

【００３７】ＩＣカード１は、共通鍵サービスに関するリーダライタ２との通信を実行する通信部５１、通信部５１の処理によって得られたデータの処理を実行する共通鍵サービス処理部５２、公開鍵サービスに関するリーダライタ２との通信を実行する通信部５３、通信部５３の処理によって得られたデータの処理を実行する公開鍵サービス処理部５４から構成されている。

【００３８】通信部５１は、非接触式共通鍵対応リーダライタ２－１と通信を行うためのコイルを備えており、通信部２１と同様に、例えば、ＩＣカード1から送信されるデータが、ＡＳＫやＢＰＳＫを用いて変調されている場合、所定の処理により、受信したデータを復調し、共通鍵サービス処理部５２の制御部６１に供給するとともに、共通鍵サービス処理部５２の処理により生成されたデータを、制御部６１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、リーダライタ２に送信する。

【００３９】共通鍵サービス処理部５２は、制御部６１、メモリ６２、および暗号処理部６３から構成されている。制御部６１は、通信部５１から供給されたデータに従って、暗号処理部６３を制御し、ＩＣカード１との認証処理等に必要な処理を実行させたり、必要に応じて、メモリ６２に記録されているデータを読み込んで、通信部５１を介して、リーダライタ２に送信する。

【００４０】メモリ６２は、図３を用いて説明したメモリ３２と同様に、メモリ領域４４、ＳＲＴ４５、およびＳＲＡ４６で構成されている。メモリ領域４４には、カードＩＤ、サービス登録用の認証鍵Kreg、および、モジュール間通信で用いられる共有秘密鍵K_commonが記録されている。

【００４１】暗号処理部６３は、共通鍵処理部４２、その他の暗号処理部４３で構成されている。すなわち、共通鍵サービス処理部５２においては、公開鍵に関するサービスを処理しないため、暗号処理部６３には、図３を用いて説明した公開鍵処理部４１は備えられていない。

【００４２】通信部５３は、非接触式公開鍵対応リーダライタ２－２、あるいは、接触式公開鍵対応リーダライタ２－３と通信を行うためのコイルもしくは接触端子を備えている。通信部５３も、通信部２１と同様に、例えば、ＩＣカード1から送信されるデータが、ＡＳＫやＢＰＳＫを用いて変調されている場合、所定の処理により、受信したデータを復調し、公開鍵サービス処理部５４の制御部６１に供給するとともに、公開鍵サービス処理部５４の処理により生成されたデータを、制御部６１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、リー

ダライタ２に送信する。

【００４３】公開鍵サービス処理部５４は、制御部６１、メモリ６２、および暗号処理部３３から構成されている。すなわち、暗号処理部６３に代わって、図３を用いて説明した暗号処理部３３が備えられている以外は、共通鍵サービス処理部と、基本的に同様の構成である。

【００４４】次に、図５を用いて、公開鍵処理部４１乃至その他の暗号処理部４３について説明する。

【００４５】図５（Ａ）に示されるように、公開鍵処理部４１には、例えば、ＲＳＡ（Rivest, Shamir, Adleman）公開鍵暗号システムを利用して署名の生成および検証を行うＲＳＡ署名生成・検証部７１や、ＤＳＡ（Digital Signature Algorithm）方式を利用して署名の生成および検証を行うＤＳＡ署名生成・検証部７２が備えられている。

【００４６】ＲＳＡ署名生成・検証部７１では、２つの鍵によって暗号化と復号を行う。ＲＳＡ暗号系では、２つの鍵は、例えば、次のようにして決められる。

【００４７】ある２つの大きな素数pとqを選んで、その積n=pqを求める。そして、（p−1）×（q−1）以下で（p−1）×（q−1）と互いに素な整数eを選び、次の式（１）を満たす整数ｄを求める。

$E \times d = 1 \bmod ((p-1) \times (q-1)) \cdots (1)$

すると（e, n）が公開鍵、ｄが秘密鍵となる。

【００４８】文Mを暗号化して、暗号化データＣを生成する場合、次の式（２）を用いる。

$C = M^{e} \bmod n \cdots (2)$

また、暗号化データＣを復号する場合、次の式（３）を用いる。

$M = C^{d} \bmod n \cdots (3)$

【００４９】ＤＳＡ署名生成・検証部７２には、図示しない乱数生成部が備えられている。ＤＳＡは、DLP（Discrete Logarithm Problem;離散対数問題）の困難性をベースとしたElGamal署名を改良して、署名の長さを160bit×2に短縮し、署名鍵の生成等を特定の方法で運用するデジタル署名アルゴリズムである。署名生成において、ハッシュ関数（データ圧縮関数）にSHA－１（Secure Hash Algorithm－1）を使うことを前提としている。ＤＳＡ方式は、米国政府機関であるNIST（米国商務省標準技術局：National Institute of Standards and Technology）により、電子署名の標準として開発され、米国連邦情報処理標準（Federal Information Processing Standard）FIPS PUB 186に定められた。

【００５０】また、図５（Ｂ）に示されるように、共通鍵処理部４２には、例えば、ＤＥＳ（Data Encryption Standard）共通鍵暗号システムによる認証処理を行うＤＥＳ処理部７３、ＲＣ５（Rivest Cipher 5）方式による認証処理を行うＲＣ５処理部７４、およびＡＥＳ（Advanced Encryption Standard）方式による認証処理を行うＡＥＳ処理部７５が備えられている。

【００５１】ＤＥＳ共通鍵暗号システムは、1977年にNISTで制定され、1981年に米国規格協会（ANSI：American National Standards Institute）により標準化された共通鍵暗号システムである。ＤＥＳ共通鍵暗号システムの鍵の認証アルゴリズムは公開されており、共通鍵暗号システムの代表として広く普及している。

【００５２】ＤＥＳ共通鍵暗号システムは、データを64bit単位に区切って暗号化および復号処理を行う暗号システムである。ＤＥＳアルゴリズムにおいては、暗号化と復号は対称をなしており、受信した暗号文を同じ鍵を使ってもう一度変換すれば元の文章が復元できる。また、ＤＥＳ共通鍵暗号システムでは、簡単なビット位置転置とXOR演算の組み合わせ論理を16回繰り返している。内部的にはデータのフィードバックや条件判断部分がなく、処理が逐次的なので、パイプライン化すれば高速に処理することができる。もともとLSI化することを前提にして決められたアルゴリズムであり、ＤＥＳチップも多く作られている。

【００５３】ＲＣ５とは、ＲＳＡ Data Security社と、マサチューセッツ工科大学が開発したRCシリーズの共通鍵暗号方式であり、1995年に提案された。ＲＣ５は、可変長ブロックサイズ、可変長の鍵サイズ、および可変長回数（元データや鍵によって、ビット回転の量が変わる、Data dependent rotations（データ依存ビット回転）アルゴリズム）のラウンドを有するブロック暗号化方式である。そのブロックサイズとしては、32、64、128ビットをとることが可能であり、ラウンド数は0から255、鍵サイズは0から2048ビットまで可変である。ＲＣ５のアルゴリズムは公開されていて、RFC2040として入手することが可能である。

【００５４】また、ＡＥＳ方式は、NISTによって選定作業が行われている、米国政府の次世代標準暗号化方式である。現在標準暗号として用いられているＤＥＳが制定されたのは1977年であり、近年のコンピュータの高性能化、暗号理論の発展に伴い、その信頼性は年々低下している。そこで、NISTはＤＥＳに代わる次世代の暗号標準として、ＡＥＳ候補となる暗号方式を全世界から公募した。世界中から集まった１５の方式が審査を受けており、２１世紀初頭までに決定される予定である。

【００５５】そして、その他の暗号処理部４３は、例えば、デジタル署名を用いる場合に、メッセージに対して、不可逆的なハッシュ関数を作用させることで、「メッセージダイジェスト」を作成し、メッセージダイジェストを署名鍵により暗号化することによって、デジタル署名を作成する等の、公開鍵処理部４１もしくは共通鍵処理部４２が処理する以外の暗号処理を実行する。その他の暗号処理部４３には、図５（Ｃ）に示されるように、例えば、署名生成および署名検証に用いられるハッシュ関数SHA-1の処理を行うSHA-1処理部７６、および相互認証プロトコルで利用される真性乱数を生成する真性

乱数生成部７７が備えられるか、あるいは、図５（Ｄ）に示されるように、署名生成および署名検証に用いられるハッシュ関数ＭＤ５の処理を行うＭＤ５処理部７８、および相互認証プロトコルで利用される擬似乱数（ある有限な桁数の数字の範囲で出来るだけランダムな数字列をもつ人工的な乱数）を生成する擬似乱数生成部７９が備えられている。

【００５６】デジタル署名においては、公開鍵暗号方式を用いるため、処理速度が遅いことが問題となるが、メッセージダイジェストを作成することによって、デジタル署名作成にかかる時間が削減される。更に、ハッシュ関数は、データの改ざんに対して大きく反応する特性を有していることから、デジタル署名を検証する際に、デジタル署名を検証鍵で復号して取り出したメッセージダイジェストと、送られてきたメッセージ本文にハッシュ関数を作用させて作成したメッセージダイジェストを比較することにより、メッセージ本文が改ざんされていないかどうかを容易に確認することができる。

【００５７】SHA-1は任意の長さのメッセージから160bitのハッシュ値を生成する一方向ハッシュ関数である。ＤＳＡ同様、NISTが開発したもので、NISTによってFIPS PUB180 に定められた。標準原案（N544）は、基本的にFIPS PUB 180に準拠したものとなっている。

【００５８】そして、ＭＤ５は、広く一般に使われているメッセージダイジェスト関数アルゴリズムのうちの１つで、RFC1321で定義されている。ＭＤ５は、32bitコンピュータ上で効率よく計算できるように、アルゴリズムが決められている。ほかにＭＤ４やＭＤ２という、類似のアルゴリズムもある。

【００５９】次に、図６を用いて、図３および図４を用いて説明したＩＣカード１のＳＲＡ４６に格納されている情報について説明する。

【００６０】ＳＲＡ４６は、ＩＣカード１を保有するユーザが、図２を用いて説明した一般リーダライタ２－１２などを用いて、複数のサービスを受けることができるようにするために、それらの複数のサービスを受けるための情報（図２を用いて説明したサービス登録用リーダライタ２－１１を用いて登録された情報）を記録するためのメモリ領域である。

【００６１】すなわち、ＳＲＡ４６には、そのＩＣカード１に登録されているサービスの情報であるService Individual Info１乃至Ｎが登録されており、それぞれのService Individual Infoには、サービスの種類を識別するためのサービスＩＤ、サービス毎に予め定められた、１つ、もしくは複数の認証用鍵情報（図６におけるService Individual Info kにおいては、１乃至ｎのｎ個の認証用鍵情報）、サービスを受けるために利用されるサービスデータ、および、鍵情報をバージョンアップするための認証鍵Kake_vupと、必要に応じて、認証鍵に対する証明書などが登録されている。

【００６２】認証用鍵情報には、例えば、認証鍵ＩＤ、鍵のレベルおよびバージョン、認証方式、および、複数の認証鍵を識別するために用いられる識別用認証鍵Kake（必要に応じて、認証鍵に対する証明書）などが含まれる。また、サービスデータには、ユーザＩＤ以外に、Service Individual Info kが、例えば、電子マネーサービスである場合、電子マネーの残高情報や累積ポイント等、Service Individual Info kが、例えば、自動改札サービスである場合、有効区間情報等が格納される。

【００６３】次に、図７を用いて、図６のService Individual Infoに登録される認証用鍵情報について説明する。

【００６４】図７（Ａ）においては、領域No. １および領域No. ２のそれぞれに対応して、認証鍵ＩＤ、鍵のバージョン、認証方式、識別用認証鍵Kake、および、必要に応じて、証明書データが登録されている。図７（Ａ）のように認証用鍵情報が登録されている場合の認証鍵識別処理については、図２０乃至図２４を用いて後述する。

【００６５】図７（Ｂ）においては、領域No. １乃至領域No. ７のそれぞれに対応して、認証鍵ＩＤ、鍵のレベル、鍵のバージョン、認証方式、識別用認証鍵Kake、および、必要に応じて、証明書データが登録されている。図７（Ｂ）のように、鍵のレベルを含んだ認証用鍵情報が登録されている場合の認証鍵識別処理については、図２７および図２８を用いて後述する。

【００６６】次に、図８を用いて、図３および図４を用いて説明したＩＣカード１のＳＲＴ４５に格納されている情報について説明する。

【００６７】ＳＲＴ４５には、ＩＤカード１に複数のサービスが登録されている場合に、あるサービスを行いながら別のサービスのサービスデータに対してアクセスを許可するためのデータが登録されている。ＳＲＴ４５は、ＩＣカード１に登録されているサービスＩＤが記載されている登録サービスＩＤフィールド（図８においては、サービスＩＤＡ乃至Ｊとして記載されている）と、それぞれのサービスＩＤに対応するパーミッション情報が記載されているパーミッション情報フィールドで構成されている。

【００６８】パーミッション情報の登録サービスＩＤフィールドには、登録されているサービスのサービスＩＤがすべて列挙されている。そして、パーミッション情報フィールドには、対応するサービスが実行されている場合に、登録サービスＩＤフィールドに記載されているサービスにアクセスすることができるサービスＩＤと、どのような処理を行うことを許可するかを示す情報が記載されている。例えば、読み出しおよび書き込みが許可されている場合、パーミッション情報として「ｒｗ」が記載され、読み出しのみ許可されている場合、パーミッション情報として「ｒｏ」が記載され、鍵のバージョンア

ップが許可されている場合、パーミッション情報として「ｖｕｐ」が記載される。「ｒｗ」と「ｒｏ」は同じサービスＩＤに対して許可されないが、「ｒｗ」と「ｖｕｐ」および「ｒｏ」と「ｖｕｐ」は、同じサービスＩＤに対して許可され、パーミッション情報フィールドに列挙することが可能である。

【００６９】すなわち、ＳＲＴ４５に、図８に示されるパーミッション情報が登録されている場合、サービスＩＤがＣで示されるサービスの実行中には、サービスＩＤがＢで示されるサービスに対して、読み出し、および書き込みが許可され、更に、サービスＩＤがＤで示されるサービスの実行中においても、サービスＩＤがＢで示されるサービスに対しての読み出しが許可され、サービスＩＤがＥで示されるサービスの実行中に、サービスＩＤがＤで示されるサービスに対して、読み出し、書き込み、および鍵のバージョンアップが許可され、以下、サービスＩＤがＥで示されるサービス、サービスＩＤがＦで示されるサービス、サービスＩＤがＧで示されるサービス、もしくは、サービスＩＤがＩで示されるサービスにおいても、対応するパーミッション情報フィールドに記載されている情報に基づいて、他のサービスＩＤに対応する処理の実行中に、パーミッション情報に対応した処理が許可される。

【００７０】これらのパーミッション情報の登録は、ＩＣカード１に、対応するサービスを登録する場合に行われる。すなわち、ユーザが、サービス登録用リーダライタ２－１１を用いて、自分自身が保有するＩＣカード１に対して、サービスＩＤがＦで示されるサービスを登録する場合、例えば、サービスＩＤがＧで示されるサービスがすでに登録され、サービスＩＤがＨで示されるサービスが登録されていないならば、登録サービスＩＤフィールドのＦに対応するパーミッション情報フィールドには、サービスＩＤがＧで示されるサービスに対応するパーミッション情報しか登録することができない。そして、ユーザが、サービスＩＤがＨで示されるサービスをＩＤカード１に登録した後、サービスＩＤがＦで示されるサービスをアップデートすることにより、サービスＩＤがＦで示されるサービスに対する、サービスＩＤがＨで示されるサービスのパーミッション情報を登録することができる。

【００７１】次に、図９は、リーダライタ２の構成を示すブロック図である。

【００７２】リーダライタ２は、ＩＣカード１との通信を行う通信部９１と、データ処理を実行するリーダライタ処理部９２から構成されている。

【００７３】通信部９１は、ＩＣカード１との通信方法によって（すなわち、リーダライタ２が、図１を用いて説明した非接触式と接触式のいずれの通信方式を採用しているかによって）、電磁波を用いて通信するためのコイルのみを備えるか、もしくは、電磁波を用いて通信するためのコイル、および接触式により通信するための接触端子を備える構造を有している。

【００７４】通信部９１は、ＩＣカード１から送信されたデータを受信し、受信したデータが、例えば、ＡＳＫやＢＰＳＫを用いて変調されている場合、所定の処理により、受信したデータを復調し、リーダライタ処理部９２の制御部１０１に供給するとともに、リーダライタ処理部９２の処理により生成されたデータを、制御部１０１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、ＩＣカード１に送信する。

【００７５】リーダライタ処理部９２は、制御部１０１、暗号処理部１０２、メモリ１０３、通信部１０４、表示部１０５、および入力部１０６より構成されている。制御部１０１は、通信部９１から供給されたデータに従って、暗号処理部１０２を制御し、ＩＣカード１との認証処理等に必要な暗号処理を実行させたり、必要に応じて、メモリ１０３に記録されているデータを読み込んで、通信部９１を介して、ＩＣカード１に送信したり、ユーザが入力部１０６を用いて入力した各種操作に対応した信号や、ネットワークを介して、通信部１０４に入力された制御信号の入力を受け、これらの信号に従って、処理を実行し、その結果を表示部１０５に表示させる。

【００７６】また、通信部１０４には、ドライブ１１４も接続されており、ドライブ１１４に装着される磁気ディスク１１５、光ディスク１１６、光磁気ディスク１１７、および半導体メモリ１１８などとデータの授受を行ことができる。

【００７７】暗号処理部１０２は、図３を用いて説明した暗号処理部３３と同様の構成を有しているので、その説明は省略する。

【００７８】メモリ１０３には、ＩＣカード１と所定の処理を実行するための情報が記憶されている。その情報は、リーダライタ２が、図２を用いて説明した、サービス登録用リーダライタ２－１１乃至バージョンアップ用リーダライタ２－１４のいずれに対応するものであるかによって異なる。図１０乃至図１４を用いて、サービス登録用リーダライタ２－１１乃至バージョンアップ用リーダライタ２－１４のメモリ１０３に記憶されているデータについて説明する。

【００７９】図１０に示される、サービス登録用リーダライタ２－１１のメモリ１０３には、ＩＣカード１のメモリ３２のＳＲＡ４６にデータを登録もしくは削除する場合に用いられる認証鍵Kregが記憶され（必要に応じて認証鍵の証明書も記憶されている）、ＩＣカード１に登録するための各種サービスに対応するService Individual Info１乃至ｎが記憶されている。

【００８０】図１１に示される、一般リーダライタ２－１２のメモリ１０３には、この一般リーダライタ２－１２で処理することが可能なサービスに対応するサービス

ＩＤと、それに対応する認証鍵リスト、および鍵失効情報が記憶されている。また、一般リーダライタ２－１２に、鍵バージョンアップのサービスを可能とさせる場合、一般リーダライタ２－１２のメモリ１０３には、新バージョンの鍵などの情報も、あわせて記憶される。

【００８１】図１２に示される、モジュール間通信用リーダライタ２－１３のメモリ１０３には、一般リーダライタ２－１２のメモリ１０３に記憶されている情報と同様に、このモジュール間通信用リーダライタ２－１３で処理することが可能なサービスに対応するサービスＩＤと、それに対応する認証鍵リスト、および鍵失効情報が記憶されている。モジュール間通信とは、図１３に示されるように、共通鍵方式および公開鍵方式の２方式に対応するようになされているモジュール間通信用リーダライタ２－１３に、公開鍵モジュール１２１（例えば、図４を用いて説明した、ＩＣカード１の通信部５３および公開鍵サービス処理部５４に対応する）と、共通鍵モジュール１２２（例えば、図４を用いて説明したＩＣカード１の通信部５１および共通鍵サービス処理部５２に対応する）を有するＩＣカード１を装着し、公開鍵モジュール１２１と共通鍵モジュール１２２とのデータの通信を、モジュール間通信用リーダライタ２－１３を介して行うことである。モジュール間通信に関する処理の詳細は、図４８乃至図５１を用いて後述する。

【００８２】そして、図１４に示される、バージョンアップ用リーダライタ２－１４のメモリ１０３には、装着されたＩＣカード１に登録されているサービスの認証鍵をバージョンアップするための、サービスＩＤと、そのサービスＩＤに対応するバージョンアップ用認証鍵Kake_vupおよび認証鍵Kakeのリストが記憶されている。

【００８３】ＩＣカード１とリーダライタ２とが通信を行う場合、いくつかの例外となる処理を除いて、はじめに、ＩＣカード１とリーダライタ２が相互認証するために、通信を行うサービスを相互に識別し、そのサービスの認証鍵を相互に識別する必要がある。図１５のフローチャートを参照して、ＩＣカード１とリーダライタ２の相互認証処理について説明する。

【００８４】まず、ステップＳ１において、リーダライタ２は、必要に応じて、ＩＣカード１と通信して必要なデータの授受を行うことにより、図１６および図１８を用いて後述するリーダライタ２のサービス識別処理を実行する。そして、ステップＳ２において、ＩＣカード１は、必要に応じて、リーダライタ２と通信して必要なデータの授受を行うことにより、図１７および図１９を用いて後述するＩＣカード１のサービス識別処理を実行する。

【００８５】そして、ステップＳ１のリーダライタ２のサービス識別処理およびステップＳ２のＩＣカード１のサービス識別処理が正常終了した場合、ステップＳ３において、リーダライタ２は、必要に応じて、ＩＣカード１と通信して必要なデータの授受を行うことにより、図２０、図２２および図２７を用いて後述するリーダライタ２の認証鍵識別処理を実行する。そして、ステップＳ４において、ＩＣカード１は、必要に応じて、リーダライタ２と通信して必要なデータの授受を行うことにより、図２１、図２３および図２８を用いて後述するＩＣカード１の認証鍵識別処理を実行する。

【００８６】次に、図１６のフローチャートを参照して、複数のサービスに対応しているＩＣカード１と、複数のサービスに対応しているリーダライタ２において、ユーザが所望のサービスを入力し、そのサービスの実行が可能か否かを判断することにより、図１５のステップＳ１において実行されるリーダライタ２のサービス識別処理について説明する。

【００８７】リーダライタ２の制御部１０１は、ステップＳ１１において、ＩＣカード１に対し、通信部９１を介して、ＩＣカード検出コマンドを送信し、ステップＳ１２において、ＩＣカード１からＡＣＫ信号（後述する図１７のステップＳ２２において、ＩＣカード１が送信した信号）を受信したか否かを判断する。ステップＳ１２において、ＡＣＫ信号が受信されていないと判断された場合、ＡＣＫ信号が受信されたと判断されるまで、ステップＳ１２の処理が繰り返される。

【００８８】ステップＳ１２において、ＡＣＫ信号を受信したと判断された場合（すなわち、ＩＣカード１が、リーダライタ２に装着された場合）、ステップＳ１３において、制御部１０１は、ユーザが入力部１０６を用いて入力した操作を示す信号に従って、または、予め決められたサービスに基づいて、ユーザが希望するサービスに対応するサービスＩＤを、通信部９１を介して、ＩＣカード１に送信する。

【００８９】ステップＳ１４において、制御部１０１は、ＩＣカード１から送信される信号（後述する図１７のステップＳ２５もしくはステップＳ２６において、ＩＣカード１が送信した信号）を受信する。ステップＳ１５において、制御部１０１は、ステップＳ１４において受信したデータは、ＡＣＫ信号か否かを判断する。ステップＳ１５において、受信した信号がＡＣＫ信号ではない（すなわちＮＡＣＫ信号である）と判断された場合、ステップＳ１６において、制御部１０１は、エラーメッセージに対応するデータを表示部１０５に出力して表示させ、処理を終了する（すなわち、処理は、図１５のステップＳ３には進まない）。ステップＳ１５において、受信した信号がＡＣＫ信号であると判断された場合、処理は、図１５のステップＳ３に進む。

【００９０】次に、図１７のフローチャートを参照して、図１５のステップＳ２において、図１６を用いて説明したリーダライタ２のサービス識別処理と並行して実行される、ＩＣカード１のサービス識別処理について説明する。なお、ここでは、図３を用いて説明したＩＣカ

ード１において処理が行われるものとして説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【００９１】ＩＣカード１の制御部３１は、ステップＳ２１において、図１６のステップＳ１１において、リーダライタ２が送信したＩＣカード検出コマンドを、通信部２１を介して受信し、ステップＳ２２において、リーダライタ２にＡＣＫ信号を送信する。

【００９２】制御部３１は、ステップＳ２３において、図１６のステップＳ１３において、リーダライタ２が送信したサービスＩＤを、通信部２１を介して受信し、ステップＳ２４において、受信したサービスＩＤは、ＩＣカード１の対応するモジュール（ここでは、図３を用いて説明したＩＣカード1における処理について説明しているので、ＩＣカード処理部２２のメモリ３２に対応するが、例えば、図4を用いて説明したＩＣカード１の場合、リーダライタ２が対応している方式により、共通鍵サービス処理部５２のメモリ６２あるいは、公開鍵サービス処理部のメモリ６２に対応する）内に登録されているＩＤであるか否か、すなわち、ステップＳ２３において受信したサービスＩＤが、図６を用いて説明したＳＲＡ４６に登録されているか否かを判断する。

【００９３】ステップＳ２４において、受信したサービスＩＤが、モジュール内に登録されていると判断された場合、ステップＳ２５において、制御部３１は、通信部２１を介して、リーダライタ２にＡＣＫ信号を送信し、処理は、図１５のステップＳ４に進む。ステップＳ２４において、受信したサービスＩＤが、モジュール内に登録されていないと判断された場合、ステップＳ２６において、制御部３１は、通信部２１を介して、リーダライタ２にＮＡＣＫ信号を送信し、処理が終了される（すなわち、図１５のステップＳ４には進まない）。

【００９４】次に、図１８のフローチャートを参照して、複数のサービスに対応しているＩＣカード１と、複数のサービスに対応しているリーダライタ２において、該当するＩＣカード１とリーダライタ２が実行可能なサービスを抽出して、リーダライタ２の表示部１０５に表示させ、それらのサービスの中から、ユーザが所望するサービスを選択させることにより、サービス識別を行う場合における、図１５のステップＳ１において実行される、リーダライタ２のサービス識別処理について説明する。

【００９５】リーダライタ２の制御部１０１は、ステップＳ３１において、サービスＩＤリスト送信コマンドを、ＩＣカード１に、通信部９１を介して送信し、ステップＳ３２において、後述する図１９のステップＳ５２において、ＩＣカード１が送信した、サービスＩＤリストを受信したか否かを判断する。ステップＳ３２において、サービスＩＤリストを受信していないと判断された場合、サービスＩＤリストを受信したと判断されるまで、ステップＳ３２の処理が繰り返される。

【００９６】ステップＳ３２において、サービスＩＤリストを受信したと判断された場合、ステップＳ３３において、制御部１０１は、受信したサービスＩＤリストに記載されているサービスＩＤは、リーダライタ２が対応しているサービスが含まれているか否か（すなわち、リーダライタ２のメモリ１０３に記憶されているサービスＩＤを含んでいるか否か）を判断する。

【００９７】ステップＳ３３において、受信したサービスＩＤリストに、リーダライタ対応サービスが含まれていると判断された場合、ステップＳ３４において、制御部１０１は、サービスＩＤリストに含まれていた対応サービスが複数であるか否かを判断する。ステップＳ３４において、対応サービスが複数ではない（すなわち１つだけである）と判断された場合、処理は、ステップＳ３７に進む。

【００９８】ステップＳ３４において、対応サービスが複数であると判断された場合、制御部１０１は、ステップＳ３５において、複数の対応サービスを表示部１０５に表示させるためのデータを生成し、表示部１０５に出力して表示させ、ステップＳ３６において、入力部１０６から、ユーザが希望するサービスの入力を受ける。あるいは、サービスそれぞれに、優先度情報を含ませておき、複数の対応サービスのうちから、優先度の最も高いサービスが自動的に選択されるようにしてもよい。

【００９９】ステップＳ３７において、制御部１０１は、ステップＳ３４において、対応サービスがただ１つであると判断された場合は、そのサービスに対応するサービスＩＤを、ステップＳ３４において、対応サービスが複数であると判断された場合は、ステップＳ３６において、ユーザが入力部１０６を用いて入力した希望するサービスに対応するサービスＩＤを、通信部９１を介して、ＩＣカード１に送信し、処理は、図１５のステップＳ３に進む。

【０１００】ステップＳ３３において、受信したサービスＩＤリストに、リーダライタ対応サービスが含まれていないと判断された場合、制御部１０１は、ステップＳ３８において、通信部９１を介して、ＩＣカード１にＮＡＣＫ信号を送信し、ステップＳ３９において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される（すなわち、処理は、図１５のステップＳ３には進まない）。

【０１０１】次に、図１９のフローチャートを参照して、図１５のステップＳ２において、図１８を用いて説明したリーダライタ２のサービス識別処理と並行して実行される、ＩＣカード１のサービス識別処理について説明する。なお、ここでは、図３を用いて説明したＩＣカード１において処理が行われるものとして説明するが、図４を用いて説明したＩＣカード１によって処理が実行

される場合においても、基本的に同様の処理が実行される。

【０１０２】ＩＣカード１の制御部３１は、ステップＳ５１において、リーダライタ２が、図１８のステップＳ３１において送信したサービスＩＤ送信コマンドを、通信部２１を介して受信し、ステップＳ５２において、自分自身が対応しているサービスＩＤリスト（すなわち、メモリ３２のＳＲＡ４６に登録されているサービスＩＤのリスト）を生成して、通信部２１を介して、リーダライタ２に送信する。

【０１０３】制御部３１は、ステップＳ５３において、リーダライタ２が、図１８のステップＳ３７もしくはステップＳ３８において、ＩＣカード１に送信したデータを、通信部２１を介して受信し、ステップＳ５４において、リーダライタ２から受信したデータはＮＡＣＫ信号か否かを判断する。ステップＳ５４において、受信した信号がＮＡＣＫ信号であると判断された場合（すなわち、受信したデータが、図１８のステップＳ３８において、リーダライタ２がＩＣカード１に送信した信号である場合）、処理が終了される（すなわち、処理は、図１５のステップＳ４には進まない）。

【０１０４】ステップＳ５４において、リーダライタ２から受信したデータはＮＡＣＫ信号ではないと判断された場合（すなわち、受信したデータが、図１８のステップＳ３７において、リーダライタ２がＩＣカード１に送信したサービスＩＤである場合）、ステップＳ５５において、制御部３１は、リーダライタ２から受信したサービスＩＤは、自分自身のメモリ３２のＳＲＡ４６に登録されているか否か判断する。

【０１０５】ステップＳ５５において、サービスＩＤが登録されていないと判断された場合、処理が終了される（すなわち、処理は、図１５のステップＳ４には進まない）。ステップＳ５５において、サービスＩＤが登録されていると判断された場合、処理は、図１５のステップＳ４に進む。

【０１０６】次に、図２０のフローチャートを参照して、図７（Ａ）を用いて説明した認証用鍵情報を用いて認証鍵識別が行われる場合、図１５のステップＳ３において実行される、リーダライタ２の認証鍵識別処理について説明する。

【０１０７】リーダライタ２の制御部１０１は、ステップＳ６１において、図１５のステップＳ１およびステップＳ２のサービス識別処理により識別されたサービスに対応するサービスＩＤ（ここでは、対応するサービスＩＤを、ＩＤ_Ｓとする）に属する認証鍵のうちの１つに対応する認証鍵ＩＤを、メモリ１０３から読み出し、通信部９１を介して、ＩＣカード１に送信し、ステップＳ６２において、後述する図２１のステップＳ７３もしくはステップＳ７５において、ＩＣカード１が送信するデータを受信する。

【０１０８】ステップＳ６３において、制御部１０１は、ステップＳ６２において、ＩＣカード１から受信したデータは、ＡＣＫ信号か否かを判断する。ステップＳ６３において、ＡＣＫ信号が受信されたと判断された場合、ステップＳ６４において、制御部１０１は、暗号処理部３３を制御して、ステップＳ６１において、暗号処理部１０２の公開鍵処理部１１１もしくは共通鍵処理部１１２のうち、ＩＣカード１に送信した認証鍵ＩＤに対応する認証鍵を用いて認証処理を行う処理部を選択して制御することにより、ＩＣカード１との相互認証処理および鍵共有処理を開始し、ＩＣカード１とセッション鍵Ksesを共有し、相互認証処理が終了した後、処理が終了される。

【０１０９】ステップＳ６３において、ＡＣＫ信号が受信されていないと判断された場合（すなわち、ＮＡＣＫ信号を受信したと判断された場合）、ステップＳ６５において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。

【０１１０】次に、図２１のフローチャートを参照して、図１５のステップＳ４において、図２０のリーダライタ２の認証鍵識別処理と並行して実行される、ＩＣカード１の認証鍵識別処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１１１】ＩＣカード１の制御部３１は、ステップＳ７１において、図２０のステップＳ６１において、リーダライタ２が送信した認証鍵ＩＤを、通信部２１を介して受信し、ステップＳ７２において、ステップＳ７１において受信した認証鍵ＩＤは、メモリ３２のＳＲＡ４６のＩＤ_Ｓに関するデータが記憶されている領域に登録されているか否かを判断する。

【０１１２】ステップＳ７２において、認証鍵ＩＤが登録されていると判断された場合、制御部３１は、ステップＳ７３において、通信部２１を介して、リーダライタ２にＡＣＫ信号を送信し、ステップＳ７４において、暗号処理部３３の公開鍵処理部４１もしくは共通鍵処理部４２のうち、リーダライタ２に指定された認証鍵による認証処理を行う方を選択して制御することにより、相互認証処理を実行し、リーダライタ２とセッション鍵Ksesを共有し、相互認証処理の終了後、処理が終了される。ステップＳ７２において、認証鍵ＩＤが登録されていないと判断された場合、ステップＳ７５において、制御部３１は、通信部２１を介して、リーダライタ２にＮＡＣＫ信号を送信し、処理が終了される。

【０１１３】図２０および図２１を用いて説明した処理においては、ＩＣカード１とリーダライタ２は、図１５のステップＳ１およびステップＳ２の処理により識別されたサービスのサービスＩＤに対応する、リーダライタ

２が指定した認証鍵により、相互認証を実行する。

【０１１４】例えば、あるサービスに対して共通鍵および公開鍵の２種類の認証鍵が用意されている場合、共通鍵に基づく認証処理により高速な処理を行うことをデフォルトとし、共通鍵のバージョンが古い場合には、公開鍵に基づいて認証処理を実施するようにしてもよい。

【０１１５】次に、図２２のフローチャートを参照して、図１５のステップＳ３において実行される、図１５のステップＳ１およびステップＳ２の処理により識別されたサービスのサービスＩＤに対応するサービスに対して、共通鍵および公開鍵の２種類の認証鍵が用意されている場合のリーダライタ２の認証鍵識別処理について説明する。

【０１１６】リーダライタ２の制御部１０１は、ステップＳ８１において、図１５のステップＳ１およびステップＳ２の処理により識別されたサービスのサービスＩＤに対応する認証鍵の、共通鍵バージョン情報要求コマンドを、通信部９１を介してＩＣカード１に送信し、ステップＳ８２において、後述する図２３のステップＳ９２において、ＩＣカード１が送信した共通鍵バージョン情報を、通信部９１を介して受信する。

【０１１７】ステップＳ８３において、制御部１０１は、ステップＳ８２において受信した共通鍵バージョン情報を基に、共通鍵バージョンが有効か否かを判断する。ステップＳ８３において、共通鍵バージョンが有効であると判断された場合、ステップＳ８４において、制御部１０１は、ＩＣカード１に、共通鍵による相互認証開始コマンドを送信し、暗号処理部１０２の共通鍵処理部１１２を制御して、共通鍵による相互認証を開始し、ＩＣカード１とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【０１１８】ステップＳ８３において、共通鍵バージョンが有効ではないと判断された場合、ステップＳ８５において、制御部１０１は、ＩＣカード１に、公開鍵による相互認証開始コマンドを送信し、暗号処理部１０２の公開鍵処理部１１１を制御して、公開鍵による相互認証を開始し、ＩＣカード１とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【０１１９】次に、図２３のフローチャートを参照して、図１５のステップＳ４において、図２２を用いて説明したリーダライタ２の認証鍵識別処理と並行して実行される、ＩＣカード１の認証鍵識別処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１２０】ＩＣカード１の制御部３１は、ステップＳ９１において、図２２のステップＳ８１において、リーダライタ２が送信した共通鍵バージョン情報要求コマンドを受信し、ステップＳ９２において、共通鍵バージョン情報を、通信部２１を介して、リーダライタ２に送信する。

【０１２１】制御部３１は、ステップＳ９３において、図２２のステップＳ８４もしくはステップＳ８５において、リーダライタ２が送信した相互認証開始コマンドを受信し、ステップＳ９４において、ステップＳ９３において受信された相互認証開始コマンドは、共通鍵による相互認証開始コマンドであるか否かを判断する。

【０１２２】ステップＳ９４において、共通鍵による相互認証開始コマンドであると判断された場合、ステップＳ９５において、制御部３１は、暗号処理部３３の共通鍵処理部４２を制御して、共通鍵による相互認証を開始し、リーダライタ２とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【０１２３】ステップＳ９４において、共通鍵による相互認証開始コマンドではない（すなわち、公開鍵による相互認証開始コマンドである）と判断された場合、ステップＳ９６において、制御部３１は、暗号処理部３３の公開鍵処理部４１を制御して、公開鍵による相互認証を開始し、リーダライタ２とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【０１２４】図２２および図２３を用いて説明した処理により、ＩＣカード１とリーダライタ２は、まず、認証速度の速い共通鍵による相互認証を実行しようとし、共通鍵による相互認証が行えない場合（例えば、対応する共通鍵のバージョンが古い場合など）、公開鍵を用いて、相互認証を実行する。

【０１２５】図２２のステップＳ８５および図２３のステップＳ９６の処理においては、公開鍵による相互認証が行われる。リーダライタ２のメモリ１０３のＳＲＡ４６には、図２４（Ａ）に示されるリーダライタ２の証明書が記憶されている。また、ＩＣカード１のメモリ３２のＳＲＡ４６には、図２４（Ｂ）に示されるＩＣカード１の証明書が記憶されている。

【０１２６】図２４（Ａ）および図２４（Ｂ）に示されるように、それぞれの証明書には、証明書のバージョン番号、認証局が割り付ける証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証局の名前、証明書の有効期限、リーダライタ２、あるいはＩＣカード１の名前（ＩＤ）、リーダライタ２の公開鍵Kpsp、あるいはＩＣカード１の公開鍵Kpu、およびメッセージ全体に、図５を用いて説明したような不可逆的なハッシュ関数（データ圧縮関数）を作用させることで、メッセージダイジェストを作成し、メッセージダイジェストを、認証局の秘密鍵Kscaにより暗号化することによって作成された、デジタル署名から構成される。

【０１２７】次に、図２５のフローチャートを参照して、署名生成処理について説明する。ここでは、楕円曲線暗号方式（楕円ＤＳＡ署名）を用いて、デジタル署名

を生成する場合について説明する。ここでは、ＩＣカード１の制御部３１が、公開鍵処理部４１のＤＳＡ署名生成・検証部７２を制御することにより実行される処理について説明するが、リーダライタ２においても、同様の処理が実行されるので、リーダライタ２の処理についての説明は省略する。

【０１２８】ステップＳ１０１において、制御部３１は、署名生成処理に必要なパラメータを認識する。すなわち、ｐを標数、ａおよびｂを楕円曲線の係数、楕円曲線を$y^2=x^3+ax+b$、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｍをメッセージ、Ｋｓを秘密鍵、ＧおよびＫｓＧを公開鍵とする。

【０１２９】公開鍵処理部４１のＤＳＡ署名生成・検証部７２は、ステップＳ１０２において、図示しない乱数生成部で、０＜ｕ＜ｒとなるｕを生成し、ステップＳ１０３において、ステップＳ１０２において生成された乱数ｕを用いて、公開鍵Ｇをｕ倍し、Ｖ＝ｕＧ＝（Ｘｖ，Ｙｖ）となるＶを算出する。

【０１３０】ＤＳＡ署名生成・検証部７２は、ステップＳ１０４において、ｃ＝Ｘｖ ｍｏｄ ｒを算出し、ステップＳ１０５において、Ｓ１０４の計算結果に基づいて、ｃ＝０であるか否かを判断する。ステップＳ１０５において、ｃ＝０であると判断された場合、処理は、ステップＳ１０２に戻り、それ以降の処理が繰り返される。

【０１３１】ステップＳ１０５において、ｃ＝０ではないと判断された場合、ＤＳＡ署名生成・検証部７２は、ステップＳ１０６において、メッセージＭのハッシュ値であるｆ＝SHA-1（Ｍ）（ここでは、ハッシュ関数として、SHA-1が用いられる）を算出し、ステップＳ１０７において、ｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ ｒを計算する。

【０１３２】ステップＳ１０８において、ＤＳＡ署名生成・検証部７２は、ステップＳ１０７の計算結果に基づいて、ｄ＝０か否かを判断する。ステップＳ１０８において、ｄ＝０であると判断された場合、処理は、ステップＳ１０２に戻り、それ以降の処理が繰り返される。ステップＳ１０８において、ｄ＝０ではないと判断された場合、ステップＳ１０９において、ＤＳＡ署名生成・検証部７２は、署名データを（ｃ，ｄ）とし、処理が終了される。

【０１３３】このようにしてＩＣカード１において生成されたデジタル署名を受信したリーダライタ２は、受信したデジタル署名を検証する処理を実施する。図２６のフローチャートを参照して、署名検証処理について説明する。ここでは、リーダライタ２の制御部１０１が、公開鍵処理部４１のＤＳＡ署名生成・検証部７２を制御することにより実行される処理について説明するが、ＩＣカード１においても、同様の処理が実行されるので、ＩＣカード１の処理についての説明は省略する。

【０１３４】ステップＳ１１１において、制御部１０１は、署名生成処理に必要なパラメータを認識する。すなわち、ｐを標数、ａおよびｂを楕円曲線の係数、楕円曲線を$y^2=x^3+ax+b$、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｍをメッセージ、Ｋｓを秘密鍵、ＧおよびＫｓＧを公開鍵とする。

【０１３５】公開鍵処理部４１のＤＳＡ署名生成・検証部７２は、ステップＳ１１２において、受信した署名データのｃおよびｄの値に基づいて、０＜ｃ＜ｒかつ０＜ｄ＜ｒであるか否かを判断する。

【０１３６】ステップＳ１１２において、０＜ｃ＜ｒかつ０＜ｄ＜ｒではないと判断された場合、処理はステップＳ１２０に進む。ステップＳ１１２において、０＜ｃ＜ｒかつ０＜ｄ＜ｒであると判断された場合、ステップＳ１１３において、ＤＳＡ署名生成・検証部７２は、メッセージＭのハッシュ値であるｆ＝SHA-1（Ｍ）を算出し、ステップＳ１１４において、ｈ＝１／ｄ ｍｏｄ ｒを計算する。

【０１３７】ＤＳＡ署名生成・検証部７２は、ステップＳ１１４において算出されたｈの値を用いて、ステップＳ１１５において、ｈ１＝ｆｈ、ｈ２＝ｃｈ ｍｏｄ ｒを算出し、ステップＳ１１６において、Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１Ｇ＋ｈ２ＫｓＧを算出する。

【０１３８】ステップＳ１１７において、ＤＳＡ署名生成・検証部７２は、ステップＳ１１６の算出結果から、Ｐの値が無限遠点であるか否かを判断する。ここでは、Ｐの値が無限遠点である場合、ステップＳ１１６において、ｈ１Ｇ＋ｈ２ＫｓＧの解を得ることができないことに基づいて、Ｐの値が無限遠点であるか否かを判断することが可能である。ステップＳ１１７において、Ｐが無限遠点であると判断された場合、処理は、ステップＳ１２０に進む。

【０１３９】ステップＳ１１７において、Ｐの値が無限遠点ではないと判断された場合、ステップＳ１１８において、ＤＳＡ署名生成・検証部７２は、ｃ＝Ｘｐ ｍｏｄ ｒが成り立つか否かを判断する。ステップＳ１１８において、ｃ＝Ｘｐ ｍｏｄ ｒが成り立たないと判断された場合、処理は、ステップＳ１２０に進む。

【０１４０】ステップＳ１１８において、ｃ＝Ｘｐ ｍｏｄ ｒが成り立つと判断された場合、ステップＳ１１９において、ＤＳＡ署名生成・検証部７２は、受信した署名は正しいと判断し、処理が終了される。

【０１４１】ステップＳ１１２において、０＜ｃ＜ｒかつ０＜ｄ＜ｒではないと判断された場合、ステップＳ１１７において、ｐが無限遠点であると判断された場合、もしくは、ステップＳ１１８において、ｃ＝Ｘｐ ｍｏｄ ｒが成り立たないと判断された場合、ステップＳ１２０において、ＤＳＡ署名生成・検証部７２は、受信した署名は正しくないと判断し、処理が終了される。

【０１４２】また、図７（Ｂ）を用いて説明した認証用鍵情報を用いて認証鍵識別が行われ、あるサービスに対

してレベル分けされた複数の認証鍵が格納されているような場合、低レベルの鍵から優先的に認証処理を開始し、その鍵のバージョンを判定し、その鍵のバージョンが古いとき、より高いレベルの認証鍵を用いて認証処理を行うようにしてもよい。

【０１４３】次に、図２７のフローチャートを参照して、図１５のステップＳ３において実行される、あるサービスに対してレベル分けされた複数の認証鍵が格納されている場合のリーダライタ２の認証鍵識別処理について説明する。

【０１４４】リーダライタ２の制御部１０１は、ステップＳ１３１において、通信部９１を介して、鍵レベル交渉コマンドを、ＩＣカード１に送信し、ステップＳ１３２において、後述する図２８のステップＳ１４３において、ＩＣカード１が送信する、レベルＮにおける鍵バージョン情報Ｖを、通信部９１を介して受信する。

【０１４５】ステップＳ１３３において、制御部１０１は、ステップＳ１３２において受信した鍵バージョン情報ＶのレベルＮは、Ｎ＞０であるか否かを判断する。ステップＳ１３３において、Ｎ＞０ではないと判断された場合、処理はステップＳ１３７に進む。

【０１４６】ステップＳ１３３において、Ｎ＞０であると判断された場合、ステップＳ１３４において、制御部１０１は、ステップＳ１３２において受信した鍵バージョン情報Ｖに基づいて、レベルＮにおける鍵バージョン情報は有効か否かを判断する。

【０１４７】ステップＳ１３４において、レベルＮにおける鍵バージョンが有効ではないと判断された場合（すなわち、鍵のバージョンが古いと判断された場合）、ステップＳ１３５において、制御部１０１は、通信部９１を介して、ＩＣカード１にＮＡＣＫ信号を送信し、処理はステップＳ１３２に戻り、それ以降の処理が繰り返される。

【０１４８】ステップＳ１３４において、レベルＮにおける鍵バージョンは有効であると判断された場合、ステップＳ１３６において、制御部１０１は、通信部９１を介して、ＩＣカード１にＡＣＫ信号を送信し、処理が終了される。

【０１４９】ステップＳ１３３において、Ｎ＞０ではないと判断された場合、ステップＳ１３７において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。

【０１５０】次に、図２８のフローチャートを参照して、図２７を用いて説明したリーダライタ２の認証鍵識別処理と並行して実行される、ＩＣカード１の認証鍵識別処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１５１】ＩＣカード１の制御部３１は、ステップＳ１４１において、図２７のステップＳ１３１において、リーダライタ２が送信した鍵レベル交渉コマンドを受信し、ステップＳ１４２において、現在の鍵レベルＮを、Ｎ＝１にセットする。

【０１５２】制御部３１は、ステップＳ１４３において、現在の鍵レベルＮと、そのレベルにおける鍵バージョン情報Ｖを、通信部２１を介して、リーダライタ２に送信し、ステップＳ１４４において、図２７のステップＳ１３５もしくはステップＳ１３６において、リーダライタ２が送信したデータを受信する。

【０１５３】ステップＳ１４５において、制御部３１は、ステップＳ１４４において、リーダライタ２から受信した信号は、ＡＣＫ信号であるか否かを判断する。ステップＳ１４５において、リーダライタ２から受信した信号はＡＣＫ信号ではないと判断された場合、制御部３１は、ステップＳ１４６において、Ｎ＝Ｎ＋１とし、ステップＳ１４７において、Ｎの値が所定の最大レベルを超えているか否かを判断する。

【０１５４】ステップＳ１４７において、Ｎが最大レベルを超えていないと判断された場合、処理はステップＳ１４３に戻り、それ以降の処理が繰り返される。ステップＳ１４７において、Ｎが最大レベルを超えていると判断された場合、ステップＳ１４８において、制御部３１は、現在のレベルをＮ＝０（Ｎ＝０は、例外状態を示すものとする）とし、処理はステップＳ１４３に戻り、それ以降の処理が繰り返される。

【０１５５】ステップＳ１４５において、リーダライタ２から受信した信号はＡＣＫ信号であると判断された場合、処理が終了される。

【０１５６】図１５乃至図２８を用いて、ＩＣカード１と、リーダライタ２のサービス識別および認証鍵識別に関する処理について説明したが、例えば、図２を用いて説明したサービス登録用リーダライタ２－１１に、ＩＣカード１を装着し、新たなサービスの登録を実行する場合、およびサービスの削除を実行する場合には、図１０を用いて説明したように、サービス登録用リーダライタ２－１１のメモリ１０３に記憶されているサービス登録用の認証鍵Kregを用いて認証処理を行うため、図１５乃至図２８を用いて説明したような相互認証処理を用いなくてもよい。

【０１５７】次に、図２９のフローチャートを参照して、サービス登録用リーダライタ２－１１のサービス登録処理について説明する。

【０１５８】サービス登録用リーダライタ２－１１の制御部１０１は、ステップＳ１５１において、通信部９１を介して、サービス登録コマンドを、ＩＣカード１に送信し、ステップＳ１５２において、ＩＣカード１と、サービス登録用鍵Kregによる相互認証を行い、セッション鍵Ksesを共有する。

【０１５９】制御部１０１は、ステップＳ１５３において、空き領域確認コマンドを、通信部９１を介してＩＣカード１に送信し、ステップＳ１５４において、後述する図３０のステップＳ１７５もしくはステップＳ１７６においてＩＣカード１から送信されるデータを受信する。

【０１６０】ステップＳ１５５において、制御部１０１は、ステップＳ１５４において、ＩＣカード１から受信した信号はＡＣＫ信号であるか否かを判断する。ステップＳ１５５において、ＩＣカード１から受信した信号がＡＣＫ信号であると判断された場合、制御部１０１は、ステップＳ１５６において、暗号処理部１０２の共通鍵処理部１１２を制御して、ＩＣカード１のメモリ３２に新たに登録する登録データを、セッション鍵Ksesで暗号化させ、ステップＳ１５７において、暗号化データを、通信部９１を介して、ＩＣカード１に送信する。

【０１６１】制御部１０１は、ステップＳ１５８において、後述する図３０のステップＳ１８０において、ＩＣカード１が送信したデータ登録完了通知を、通信部９１を介して受信し、ステップＳ１５９において、サービス認証によるサービス削除許可フラグを送信し、処理が終了される。

【０１６２】ステップＳ１５５において、ＩＣカード１から受信した信号がＡＣＫ信号ではないと判断された場合、ステップＳ１６０において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。

【０１６３】次に、図３０のフローチャートを参照して、図２９を用いて説明した、サービス登録用リーダライタ２－１１のサービス登録処理と並行して実行される、ＩＣカード１のサービス登録処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１６４】ステップＳ１７１において、ＩＣカード１の制御部３１は、通信部２１を介して、図２９のステップＳ１５１において、サービス登録用リーダライタ２－１１が送信したサービス登録コマンドを受信する。

【０１６５】制御部３１は、ステップＳ１７２において、ＩＣカード１と、サービス登録用鍵Kregによる相互認証を行い、セッション鍵Ksesを共有し、ステップＳ１７３において、通信部２１を介して、図２９のステップＳ１５３において、サービス登録用リーダライタ２－１１が送信した、空き領域確認コマンドを受信する。

【０１６６】ステップＳ１７４において、制御部３１は、メモリ３２のＳＲＡ４６に、登録データ用の空き領域があるか否かを判断する。ステップＳ１７４において、空き領域がないと判断された場合、ステップＳ１７５において、制御部３１は、サービス登録用リーダライタ２－１１に、通信部２１を介して、ＮＡＣＫ信号を送信し、処理が終了される。

【０１６７】ステップＳ１７４において、空き領域があると判断された場合、ステップＳ１７６において、制御部３１は、サービス登録用リーダライタ２－１１に、通信部２１を介して、ＡＣＫ信号を送信する。

【０１６８】制御部３１は、ステップＳ１７７において、図２９のステップＳ１５７において、サービス登録用リーダライタ２－１１が送信した暗号化データを、通信部２１を介して受信し、ステップＳ１７８において、暗号処理部３３の共通鍵処理部４２を制御して、ステップＳ１７７において受信した暗号化データを、セッション鍵Ksesを用いて復号させる。

【０１６９】ステップＳ１７９において、制御部３１は、ステップＳ１７８において、セッション鍵Ksesにより復号されたデータを、メモリ３２に供給し、ＳＲＡ４６のService Individual Info領域およびＳＲＴ４５に登録させる。

【０１７０】制御部３１は、ステップＳ１８０において、データの登録完了を、通信部２１を介して、サービス登録用リーダライタ２－１１に通知し、ステップＳ１８１において、図２９のステップＳ１５９において、サービス登録用リーダライタ２－１１が送信した、サービス認証によるサービス削除許可フラグを受信し、サービス削除許可フラグを、メモリ３２のＳＲＡ４６のService Individual Info領域に設定し、処理が終了される。

【０１７１】次に、図３１のフローチャートを参照して、サービス登録用リーダライタ２－１１のサービス削除処理について説明する。

【０１７２】ステップＳ１９１において、サービス登録用リーダライタ２－１１の制御部１０１は、ユーザが、入力部１０６を用いて入力した、削除するサービスに対応するサービスＩＤの入力を受ける（ここでは、対応するサービスＩＤが、ＩＤ_Ｓであるサービスが削除されるものとする）。

【０１７３】ステップＳ１９２において、図２９のステップＳ１５２と同様の処理がなされる。制御部１０１は、ステップＳ１９３において、通信部９１を介して、ＩＣカード１に、ＩＤ_Ｓ領域削除コマンドを送信し、ステップＳ１９４において、後述する図３２のステップＳ２０５においてＩＣカード１が送信した、エラーメッセージを受信したか否かを判断する。

【０１７４】ステップＳ１９４において、エラーメッセージを受信したと判断された場合、ステップＳ１９５において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。ステップＳ１９４において、エラーメッセージを受信しなかったと判断された場合、処理が終了される。

【０１７５】次に、図３２のフローチャートを参照して、図３１を用いて説明した、サービス登録用リーダラ

イタ２－１１のサービス削除処理と並行して実行される、ＩＣカード１のサービス削除処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１７６】ステップＳ２０１において、図３０のステップＳ１７２と同様の処理が実行される。ＩＣカード１の制御部３１は、ステップＳ２０２において、図３１のステップＳ１９３において、サービス登録用リーダライタ２－１１が送信した、ＩＤ_Ｓ領域削除コマンドを受信し、ステップＳ２０３において、ＩＤ_Ｓ領域に対応するデータがあるか否かを確認することなどにより、ステップＳ２０２において受信したＩＤ_Ｓ領域削除コマンドの正当性が検証されたか否かを判断する。

【０１７７】ステップＳ２０３において、ＩＤ_Ｓ領域削除コマンドの正当性が検証されたと判断された場合、ステップＳ２０４において、制御部３１は、メモリ３２のＳＲＴ４５およびＳＲＡ４６から、ＩＤ_Ｓに対応する領域を削除し、処理が終了される。

【０１７８】ステップＳ２０３において、ＩＤ_Ｓ領域削除コマンドの正当性が検証されなかったと判断された場合、ステップＳ２０５において、制御部３１は、通信部２１を介して、サービス登録用リーダライタ２－１１に、エラーメッセージを送信し、処理が終了される。

【０１７９】図３１および図３２を用いて説明したサービス削除処理は、一般リーダライタ２－１２とＩＣカード１とで実行することも可能である。図３３のフローチャートを参照して、一般リーダライタ２－１２のサービス削除処理について説明する。

【０１８０】ステップＳ２１１において、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理が実行され、ステップＳ２１２において、図２０、図２２、もしくは図２７を用いて説明したリーダライタ２の認証鍵識別処理が実行され、ステップＳ２１３において、図３１のステップＳ１９３と同様の処理が実行される。

【０１８１】ステップＳ２１４において、一般リーダライタ２－１２の制御部１０１は、後述する図３４のステップＳ２２７もしくはステップＳ２２８において、ＩＣカード１が送信する信号を受信する。そして、ステップＳ２１５およびステップＳ２１６において、図１６のステップＳ１５およびステップＳ１６と同様の処理が実行され、処理が終了される。

【０１８２】次に、図３４のフローチャートを参照して、図３３を用いて説明した、一般リーダライタ２－１２のサービス削除処理と並行して実行される、ＩＣカード１のサービス削除処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１８３】ステップＳ２２１において、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理が実行され、ステップＳ２３２において、図２１、図２３、もしくは図２８を用いて説明したＩＣカード１の認証鍵識別処理が実行される。

【０１８４】ステップＳ２２３において、制御部３１は、図３３のステップＳ２１３において、一般リーダライタ２－１２が送信した、ＩＤ_Ｓ領域削除コマンドを、通信部２１を介して受信する。ステップＳ２２４において、図３２のステップＳ２０３と同様の処理が実行される。

【０１８５】ステップＳ２２４において、コマンドの正当性が検証されなかったと判断された場合、処理は、ステップＳ２２８に進む。ステップＳ２２４において、コマンドの正当性が検証されたと判断された場合、ステップＳ２２５において、制御部３１は、メモリ３２のＳＲＡ４６のService Individual Info領域に、サービス削除許可フラグが設定されているか否かを判断する。

【０１８６】ステップＳ２２５において、サービス削除許可フラグが設定されていないと判断された場合、処理は、ステップＳ２２８に進む。ステップＳ２２５において、サービス削除許可フラグが設定されていると判断された場合、ステップＳ２２６において、図３２のステップＳ２０４と同様の処理がなされ、ステップＳ２２７において、制御部３１は、通信部２１を介して、一般リーダライタ２－１２にＡＣＫ信号を送信し、処理が終了される。

【０１８７】ステップＳ２２４において、コマンドの正当性が検証されなかったと判断された場合、もしくは、ステップＳ２２５において、サービス削除許可フラグが設定されていないと判断された場合、ステップＳ２２８において、制御部３１は、通信部２１を介して、一般リーダライタ２－１２にＮＡＣＫ信号を送信し、処理が終了される。

【０１８８】次に、図３５のフローチャートを参照して、ユーザが、一般リーダライタ２－１２で、ＩＣカード１に登録されているサービスを受ける場合に実行される、一般リーダライタ２－１２のサービス取得処理について説明する。

【０１８９】ステップＳ２３１において、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理が実行され、ステップＳ２３２において、図２０、図２２、もしくは図２７を用いて説明したリーダライタ２の認証鍵識別処理が実行される。

【０１９０】ステップＳ２３３において、一般リーダライタ２－１２の制御部１０１は、通信部９１を介して、ＩＣカード１に、ＩＤ_Ｓ領域のデータ要求コマンドを

送信する。

【０１９１】制御部１０１は、ステップＳ２３４において、後述する図３６のステップＳ２４５において、ＩＣカード１から送信されるデータを受信し、ステップＳ２３５において、暗号処理部１０２の共通鍵処理部１１２を制御して、ステップＳ２３４において受信した暗号化データを、セッション鍵Ksesを用いて復号させる。制御部１０１は、復号されたデータを用いて、例えば、電子マネーの減算や加算などの所定のデータ処理を行い、処理が終了される。

【０１９２】次に、図３６のフローチャートを参照して、図３５を用いて説明した、一般リーダライタ２－１２のサービスデータ取得処理と並行して実行される、ＩＣカード１のサービスデータ取得処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１９３】ステップＳ２４１において、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理が実行され、ステップＳ２３２において、図２１、図２３、もしくは図２８を用いて説明したＩＣカード１の認証鍵識別処理が実行される。

【０１９４】ステップＳ２４３において、ＩＣカード１の制御部３１は、通信部２１を介して、図３５のステップＳ２３３において、一般リーダライタ２－１２が送信した、ＩＤ_Ｓ領域のデータ要求コマンドを受信する。制御部３１は、ステップＳ２４４において、暗号処理部３３の共通鍵処理部４２を制御して、メモリ３２のＩＤ_Ｓに対応する領域に登録しているデータを、セッション鍵Ksesを用いて暗号化させ、ステップＳ２４５において、通信部２１を介して、暗号化したデータを一般リーダライタ２－１２に送信し、処理が終了される。

【０１９５】また、ＩＣカード１と一般リーダライタ２－１２において、あるサービスに関する情報の授受がなされている場合においても、図８を用いて説明したＳＲＴ４５に、対応するパーミッション情報が記録されている場合、現在情報の授受がなされている以外のサービスに関する情報の授受を行うことが可能である。図３７のフローチャートを参照して、ＩＤ_Ｓ以外のサービスＩＤに対応するサービスの実行中に行われる、一般リーダライタ２－１２のサービスデータ取得処理について説明する。

【０１９６】ステップＳ２５１乃至ステップＳ２５４において、図３５のステップＳ２３１乃至ステップＳ２３４と同様の処理が実行される。ステップＳ２５５において、一般リーダライタ２－１２の制御部１０１は、ステップＳ２５４において、ＩＣカード１から受信したデータは、ＮＡＣＫ信号か否かを判断する。

【０１９７】ステップＳ２５５において、受信したデータがＮＡＣＫ信号ではないと判断された場合、ステップＳ２５６において、図３５のステップＳ２３５と同様の処理が実行され、処理が終了される。ステップＳ２５５において、受信したデータがＮＡＣＫ信号であると判断された場合、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。

【０１９８】次に、図３８のフローチャートを参照して、図３７を用いて説明した、一般リーダライタ２－１２のサービスデータ取得処理と並行して実行される、ＩＣカード１のサービスデータ取得処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１９９】ステップＳ２６１乃至ステップＳ２６３において、図３４のステップＳ２４１乃至ステップＳ２４３と同様の処理が実行される。なお、ステップＳ２６１では、サービスＩＤ_Ｓとは異なる、サービスＩＤ_Ｔの認証が行われるものとする。ステップＳ２６４において、ＩＣカード１の制御部３１は、メモリ３２のＳＲＴ４５およびＳＲＡ４６に、ステップＳ２６３において受信したデータ要求コマンドに対応するＩＤ_Ｓ領域が登録されているか否かを判断する。ステップＳ２６４において、ＩＤ_Ｓ領域が登録されていないと判断された場合、処理は、ステップＳ２６９に進む。

【０２００】ステップＳ２６４において、ＩＤ_Ｓ領域が登録されていると判断された場合、制御部３１は、ステップＳ２６５において、メモリ３２のＳＲＴ４５の、ＩＤ_Ｓに対応するパーミッション情報フィールドから、ＩＤ_Ｓのパーミッション情報を取得し、ステップＳ２６６において、ＩＤ_Ｔ認証時に、ＩＤ_Ｓのデータの読み込みが許可されているか否かを判断する（すなわち、ＳＲＴ４５のＩＤ_Ｓに対応するパーミッション情報フィールドに、ＩＤ_Ｔによる認証時に、データの読み出し許可、すなわち、ｒｏもしくはｒｗが記載されているか否かを判断する）。ステップＳ２６６において、データの読み込みが許可されていないと判断された場合、処理はステップＳ２６９に進む。

【０２０１】ステップＳ２６６において、データの読み込みが許可されていると判断された場合、ステップＳ２６７およびステップＳ２６８において、図３６のステップＳ２４４およびステップＳ２４５と同様の処理が実行され、処理が終了される。

【０２０２】ステップＳ２６４において、ＩＤ_Ｓ領域が登録されていないと判断された場合、もしくは、ステップＳ２６６において、データの読み込みが許可されていないと判断された場合、ステップＳ２６９において、制御部３１は、通信部２１を介して、一般リーダライタ

２－１２にＮＡＣＫ信号を送信し、処理が終了される。

【０２０３】図３５乃至図４８を用いて説明したサービスデータ取得処理によって、ＩＣカード１から一般リーダライタ２－１２にデータが取得され、所定の処理がなされたあと、一般リーダライタ２－１２は、必要に応じて、ＩＣカード１のメモリ３２のＳＲＴ４５もしくはＳＲＡ４６の所定の領域に対して、データを書き込む処理を実行する。

【０２０４】次に、図３９のフローチャートを参照して、一般リーダライタ２－１２のサービスデータ書き込み処理について説明する。

【０２０５】ステップＳ２８１において、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理が実行され、ステップＳ２８２において、図２０、図２２、もしくは図２７を用いて説明したリーダライタ２の認証鍵識別処理が実行される。

【０２０６】一般リーダライタ２－１２の制御部１０１は、ステップＳ２８３において、ＩＣカード１のメモリ３２に書き込むために、ＩＣカード１に送信するデータを、暗号処理部１０２の共通鍵処理部１１２を制御して、セッション鍵Ksesを用いて暗号化させ、ステップＳ２８４において、ＩＣカード１に、データ書き込みコマンドと、ステップＳ２８４において暗号化したデータを、通信部９１を介して送信し、処理が終了される。

【０２０７】次に、図４０のフローチャートを参照して、図３９を用いて説明した、一般リーダライタ２－１２のサービスデータ書き込み処理と並行して実行される、ＩＣカード１のサービスデータ書き込み処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０２０８】ステップＳ２９１において、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理が実行され、ステップＳ２３２において、図２１、図２３、もしくは図２８を用いて説明したＩＣカード１の認証鍵識別処理が実行される。

【０２０９】ステップＳ２９３において、制御部３１は、通信部２１を介して、図３９のステップＳ２８４において、一般リーダライタ２－１２が送信した、データ書き込みコマンドと暗号化データを受信する。制御部３１は、ステップＳ２９４において、暗号処理部３３の共通鍵処理部４２を制御して、受信したデータを、セッション鍵Ksesを用いて復号させ、ステップＳ２９５において、復号したデータを、メモリ３２のＳＲＴ４５およびＳＲＡ４６のＩＤ_Ｓに対応するサービス格納領域へ書き込み、処理が終了される。

【０２１０】また、ＩＣカード１と一般リーダライタ２－１２において、あるサービスに関する情報の授受がなされている場合においても、図８を用いて説明したＳＲＴ４５に、対応するパーミッション情報が記録されている場合、図３７および図３８を用いて説明したサービスデータ取得処理と同様に、現在情報の授受がなされている以外のサービスに関するサービスデータ書き込み処理を実行することが可能である。図４１のフローチャートを参照して、ＩＤ_Ｓ以外のサービスＩＤに対応するサービスの実行中に行われる、一般リーダライタ２－１２のサービスデータ書き込み処理について説明する。

【０２１１】ステップＳ３０１乃至ステップＳ３０４において、図３９のステップＳ２８１乃至ステップＳ２８４と同様の処理が実行される。そして、ステップＳ３０５およびステップＳ３０６において、図１６のステップＳ１５およびステップＳ１６と同様の処理がなされ、処理が終了される。

【０２１２】次に、図４２のフローチャートを参照して、図４１を用いて説明した、一般リーダライタ２－１２のサービスデータ書き込み処理と並行して実行される、ＩＣカード１のサービスデータ書き込み処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０２１３】ステップＳ３１１乃至ステップＳ３１３において、図４０のステップＳ２９１乃至ステップＳ２９３と同様の処理が実行される。なお、ステップＳ３１１では、サービスＩＤ_Ｓとは異なる、サービスＩＤ_Ｔの認証が行われるものとする。ステップＳ３１４およびステップＳ３１５において、図３８のステップＳ２６４およびステップＳ２６５と同様の処理がなされ、ステップＳ３１４において、ＩＤ_Ｓ領域が登録されていないと判断された場合、処理は、ステップＳ３２０に進む。

【０２１４】ステップＳ３１６において、制御部３１は、ＩＤ_Ｔ認証時に、ＩＤ_Ｓのサービスに対して、データの書き込みが許可されているか否かを判断する（すなわち、ＳＲＴ４５のＩＤ_Ｓに対応するパーミッション情報フィールドに、ＩＤ_Ｔ認証時のデータの書き込み許可、すなわち、ｒｗが記載されているか否かを判断する）。ステップＳ３１６において、データの書き込みが許可されていないと判断された場合、処理はステップＳ３２０に進む。

【０２１５】ステップＳ３１６において、データの書き込みが許可されていると判断された場合、ステップＳ３１７およびステップＳ３１８において、図４０のステップＳ２９４およびステップＳ２９５と同様の処理が実行される。ステップＳ３１９において、制御部３１は、通信部２１を介して、一般リーダライタ２－１２にＡＣＫ信号を送信し、処理が終了される。

【０２１６】ステップＳ３１４において、ＩＤ_Ｓ領域

が登録されていないと判断された場合、もしくは、ステップＳ３１６において、データの書き込みが許可されていないと判断された場合、ステップＳ３２０において、制御部３１は、通信部２１を介して、一般リーダライタ２－１２にＮＡＣＫ信号を送信し、処理が終了される。

【０２１７】以上説明したように、一般リーダライタ２－１２に、ＩＣカード１を装着し、各種サービスを受けるためには、サービス毎に定められた共通鍵、もしくは公開鍵を用いて認証処理を行わなければならない。これらの認証鍵は、セキュリティの維持のために、しばしばバージョンアップされる（すなわち、鍵が変更される）。ユーザは、図２を用いて説明したバージョンアップ用リーダライタ２－１４、もしくは一般リーダライタ２－１２に、ＩＣカード１を装着し、図４３乃至図４７を用いて後述する鍵バージョンアップ処理を実行させることにより、自分自身が管理しているＩＣカード１に登録されている認証鍵を、できるだけ最新に近いバージョンの認証鍵にバージョンアップするようにしなければならない。

【０２１８】次に、図４３を参照して、サービス毎に定められたバージョンアップ用鍵（図６および図１４を用いて説明したバージョンアップ用鍵Kake_vup）を用いて実行される、バージョンアップ用リーダライタ２－１４の鍵バージョンアップ処理について説明する。

【０２１９】ステップＳ３３１において、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理が実行され、ステップＳ３３２において、図２０、図２２、もしくは図２７を用いて説明したリーダライタ２の認証鍵識別処理が実行される。

【０２２０】ステップＳ３３３において、バージョンアップ用リーダライタ２－１４の制御部１０１は、暗号処理部１０２の共通鍵処理部１１２を制御して、バージョンアップを行う認証鍵に対応する認証鍵ＩＤを、セッション鍵Ksesを用いて暗号化させ、ＩＣカード１に送信する。ステップＳ３３４において、制御部１０１は、後述する図４４のステップＳ３５５もしくはステップＳ３６０において、ＩＣカード１が送信する信号を受信する。

【０２２１】ステップＳ３３５において、制御部１０１は、ステップＳ３３４においてＩＣカード１から受信した信号はＡＣＫ信号であるか否かを判断する。ステップＳ３３５において、受信した信号がＡＣＫ信号ではないと判断された場合、処理は、ステップＳ３３９に進む。ステップＳ３３５において、受信した信号がＡＣＫ信号であると判断された場合、ステップＳ３３６において、制御部１０１は、バージョンアップを行う認証鍵に対応する最新バージョン情報と、認証鍵Kakeをメモリ１０３から読み出し、暗号処理部１０２の共通鍵処理部１１２を制御して、セッション鍵Ksesを用いて暗号化させ、通信部９１を介して、ＩＣカード１に送信する。

【０２２２】そして、ステップＳ３３７において、ＩＣカード１が、後述する４４のステップＳ３５９もしくはステップＳ３６０において送信した信号を受信する。ステップＳ３３８において、ステップＳ３３５と同様の処理がなされ、ステップＳ３３８において、受信した信号がＡＣＫ信号であると判断された場合、処理が終了される。ステップＳ３３５およびステップＳ３３８において、受信した信号がＡＣＫ信号ではないと判断された場合、ステップＳ３３９において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。

【０２２３】次に、図４４のフローチャートを参照して、図４３を用いて説明した、バージョンアップ用リーダライタ２－１４の鍵バージョンアップ処理と並行して実行される、ＩＣカード１の鍵バージョンアップ処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０２２４】ステップＳ３５１において、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理が実行され、ステップＳ３５２において、図２１、図２３、もしくは図２８を用いて説明したＩＣカード１の認証鍵識別処理が実行される。

【０２２５】ステップＳ３５３において、制御部３１は、通信部２１を介して、図４３のステップＳ３３３において、バージョンアップ用リーダライタ２－１４が送信した、暗号化された認証鍵ＩＤを受信し、暗号処理部３３の共通鍵処理部４２を制御して、受信したデータを、セッション鍵Ksesを用いて復号させる。ステップＳ３５４において、制御部３１は、復号したデータを基に、メモリ３２のＳＲＴ４５およびＳＲＡ４６のＩＤ_Ｓに、対応する認証鍵ＩＤが存在するか否かを判断する。ステップＳ３５４において、認証鍵ＩＤが存在しないと判断された場合、処理は、ステップＳ３６０に進む。

【０２２６】ステップＳ３５４において、認証鍵ＩＤが存在すると判断された場合、制御部３１は、ステップＳ３５５において、通信部２１を介して、バージョンアップ用リーダライタ２－１４に、ＡＣＫ信号を送信し、ステップＳ３５６において、図４３のステップＳ３３６において、バージョンアップ用リーダライタ２－１４が送信した、暗号化された最新バージョン情報と認証鍵Kakeを、通信部２１を介して受信し、暗号処理部３３の共通鍵処理部４２を制御して、受信したバージョン情報を、セッション鍵Ksesを用いて復号させる。

【０２２７】ステップＳ３５７において、制御部３１は、復号したデータを基に、受信したバージョン情報は正しいか否か（すなわち、自分自身がすでに保有している認証鍵のバージョン情報より新しいバージョンであるか否か）を判断する。ステップＳ３５７において、バー

ジョン情報が正しくないと判断された場合、処理は、ステップＳ３６０に進む。

【０２２８】ステップＳ３５７において、バージョン情報は正しいと判断された場合、制御部３１は、暗号処理部３３の共通鍵処理部４２を制御して、認証鍵Kakeを、セッション鍵Ksesを用いて復号させ、メモリ３２のＳＲＡ４６における、認証鍵Kakeが記載される領域に書き込み、ステップＳ３５９において、バージョンアップ用リーダライタ２－１４に、通信部２１を介してＡＣＫ信号を送信し、処理が終了される。

【０２２９】ステップＳ３５４において、認証鍵ＩＤが存在しないと判断された場合、およびステップＳ３５７において、バージョン情報が正しくないと判断された場合、ステップＳ３６０において、制御部３１は、バージョンアップ用リーダライタ２－１４に、通信部２１を介してＮＡＣＫ信号を送信し、処理が終了される。

【０２３０】また、ＩＣカード１と一般リーダライタ２－１２において、あるサービスに関する情報の授受がなされている場合において、図８を用いて説明したＳＲＴ４５に、対応するパーミッション情報が記録されている場合、図３７および図３８を用いて説明したサービスデータ取得処理や、図４１および図４２を用いて説明したサービスデータ書き込み処理と同様に、現在情報の授受がなされている以外のサービスに関する鍵バージョンアップ処理を実行することが可能である。図４５のフローチャートを参照して、ＩＤ_Ｓ以外のサービスＩＤに対応するサービスの実行中に行われる、一般リーダライタ２－１２の鍵バージョンアップ処理について説明する。

【０２３１】ステップＳ３７１およびステップＳ３７２において、図４４のステップＳ３３１およびステップＳ３３２と同様の処理が実行される。そして、一般リーダライタ２－１２の制御部１０１は、ステップＳ３７３において、ＩＤ_Ｓに対応するサービスの認証鍵のバージョンアップコマンドを、通信部９１を介してＩＣカード１に送信し、ステップＳ３７４において、後述する図４６のステップＳ３９７もしくは図４７のステップＳ４０５において、ＩＣカード１が送信するデータを受信し、ステップＳ３７５において、ＩＣカード１から受信した信号は、ＡＣＫ信号か否かを判断する。

【０２３２】ステップＳ３７５において、受信した信号がＡＣＫ信号でないと判断された場合、処理は、ステップＳ３８２に進む。ステップＳ３７５において、受信した信号がＡＣＫ信号であると判断された場合、ステップＳ３７６乃至ステップＳ３８２において、図４３のステップＳ３３３乃至ステップＳ３３９と同様の処理がなされ、処理が終了される。

【０２３３】次に、図４６および図４７のフローチャートを参照して、図４５を用いて説明した、バージョンアップ用リーダライタ２－１４の鍵バージョンアップ処理と並行して実行される、ＩＣカード１の鍵バージョンアップ処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０２３４】ステップＳ３９１およびステップＳ３９２において、図４４のステップＳ３５１およびステップＳ３５２と同様の処理が実行される。なお、ステップＳ３９１では、サービスＩＤ_Ｓとは異なる、サービスＩＤ_Ｔの認証が行われるものとする。ステップＳ３９３において、制御部３１は、図４５のステップＳ３７３において、バージョンアップ用リーダライタ２－１４が送信した、ＩＤ_Ｓの認証鍵のバージョンアップコマンドを受信する。

【０２３５】ステップＳ３９４およびステップＳ３９５において、図３８のステップＳ２６４およびステップＳ２６５と同様の処理がなされ、ステップＳ３９４において、ＩＤ_Ｓ領域が登録されていないと判断された場合、処理は、ステップＳ４０５に進む。

【０２３６】ステップＳ３９６において、制御部３１は、ＩＤ_Ｔ認証時に、ＩＤ_Ｓの認証鍵のバージョンアップが許可されているか否かを判断する（すなわち、ＳＲＴ４５のＩＤ_Ｓに対応するパーミッション情報フィールドに、ＩＤ_Ｔ認証時のｖｕｐの許可が記載されているか否かを判断する）。ステップＳ３９６において、認証鍵のバージョンアップが許可されていないと判断された場合、処理は、ステップＳ４０５に進む。

【０２３７】ステップＳ３９６において、認証鍵のバージョンアップが許可されていると判断された場合、ステップＳ３９７において、制御部３１は、通信部２１を介して、バージョンアップ用リーダライタ２－１４に、ＡＣＫ信号を送信する。

【０２３８】そして、ステップＳ３９８乃至ステップＳ４０５において、図４４のステップＳ３５３乃至ステップＳ３６０と同様の処理が実行され、処理が終了される。

【０２３９】次に、図４８乃至図５１のフローチャートを参照して、図１３を用いて説明したモジュール間通信について説明する。モジュール間通信は、図４を用いて説明したＩＣカード１と、モジュール間通信用リーダライタ２－１３によって実行される。ここでは、図４を用いて説明したＩＣカード１の通信部５１および共通鍵サービス処理部５２を、図１３を用いて説明した共通鍵モジュール１２２とし、図４を用いて説明した通信部５３および公開鍵サービス処理部５４を、図１３を用いて説明した公開鍵モジュール１２１として説明する。

【０２４０】まず、図４８のフローチャートを参照して、共通鍵モジュール１２２が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵と、公開鍵モジュール１２１が、モジュール間通信用リーダライタ

２－１３と共有するセッション鍵とが異なる場合におけるモジュール間通信について説明する。

【０２４１】ステップＳ４１１において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４１２において、ＩＣカード１の公開鍵モジュール１２１は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、公開鍵モジュール１２１の間で、セッション鍵Kses１を共有する。

【０２４２】ステップＳ４１３において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４１４において、ＩＣカード１の共通鍵モジュール１２２は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、共通鍵モジュール１２２の間で、セッション鍵Kses２を共有する。

【０２４３】ステップＳ４１５において、モジュール間通信用リーダライタ２－１３の制御部１０１は、ステップＳ４１１およびステップＳ４１３において実行されたリーダライタ２のサービス識別処理において得られたＩＣカード１のカードＩＤを基に、公開鍵モジュール１２１と、共通鍵モジュール１２２の２つのカードＩＤが一致したか否かを判断する。ステップＳ４１５において、カードＩＤが一致しないと判断された場合、ステップＳ４１６において、図１６のステップＳ１６と同様の処理が実行される。

【０２４４】ステップＳ４１５において、２つのカードＩＤが一致すると判断された場合、ステップＳ４１７において、モジュール間通信用リーダライタ２－１３の制御部１０１は、モジュールデータ移動コマンドを公開鍵モジュール１２１に送信する。

【０２４５】公開鍵モジュール１２１の制御部６１は、ステップＳ４１８において、モジュールデータ移動開始コマンドをモジュール間通信用リーダライタ２－１３から受信し、暗号処理部３３の、共通鍵処理部４２を制御して、移動するデータをセッション鍵Kses１で暗号化させ、ステップＳ４１９で、暗号化データをモジュール間通信用リーダライタ２－１３に送信する。

【０２４６】モジュール間通信用リーダライタ２－１３の制御部１０１は、ステップＳ４２０において、暗号処理部１０２の、共通鍵処理部１１２を制御して、受信したデータをセッション鍵Kses１で復号し、ステップＳ４２１において、データをセッション鍵Kses２で暗号化させ、共通鍵モジュール１２２に送信する。共通鍵モジュール１２２の制御部６１は、ステップＳ４２２において、暗号処理部６３の、共通鍵処理部４２を制御して、受信したデータをセッション鍵Kses２で復号させ、ステップＳ４２３において、復号したデータをメモリ６２の対応する領域に保存して利用する。

【０２４７】次に、図４９のフローチャートを参照して、共通鍵モジュール１２２が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵と、公開鍵モジュール１２１が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵とが同一である場合におけるモジュール間通信について説明する。

【０２４８】ステップＳ４３１において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４３２において、ＩＣカード１の公開鍵モジュール１２１は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、公開鍵モジュール１２１の間で、セッション鍵Kses１を共有する。

【０２４９】ステップＳ４３３において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４３４において、ＩＣカード１の共通鍵モジュール１２２は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、共通鍵モジュール１２２の間で、セッション鍵Kses１を共有する。

【０２５０】ステップＳ４３５乃至ステップＳ４３９において、図４８のステップＳ４１５乃至ステップＳ４１９と同様の処理が実行される。そして、ステップＳ４４０において、モジュール間通信用リーダライタ２－１３の制御部１０１は、受信したデータを、共通鍵モジュール１２２に送信する。図４８のステップＳ４２０およびステップＳ４２１においては、受信したデータをセッション鍵Kses１で復号し、復号したデータをセッション鍵Kses２で暗号化した後に共通鍵モジュール１２２に送信したが、ここでは、共通鍵モジュール１２２も、セッション鍵Kses１を有しているため、これらの処理が必要なくなる。

【０２５１】共通鍵モジュール１２２の制御部６１は、ステップＳ４１１において、暗号処理部６３を制御して、受信したデータをセッション鍵Kses１で復号し、ステップＳ４２２において、復号したデータをメモリ６２の対応する領域に保存して利用する。

【０２５２】次に、図５０のフローチャートを参照して、共通鍵モジュール１２２が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵と、公開鍵モジュール１２１が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵とが異なるが、モジュール間通信用リーダライタ２－１３が、共通鍵モジュー

ル１２２が有するセッション鍵を、公開鍵モジュール１２１が有するもう一方のセッション鍵で暗号化し、公開鍵モジュール１２１に供給するようになされている場合におけるモジュール間通信について説明する。

【０２５３】ステップＳ４５１乃至ステップＳ４５６において、図４８のステップＳ４１１乃至ステップＳ４１６と同様の処理が実行される。すなわち、モジュール間リーダライタ２－１３と、公開鍵モジュール１２１の間で、セッション鍵Kses１が共有され、モジュール間リーダライタ２－１３と、共通鍵モジュール１２２の間で、セッション鍵Kses２が共有される。

【０２５４】ステップＳ４５７において、モジュール間通信用リーダライタ２－１３の制御部１０１は、暗号処理部１０２を制御して、セッション鍵Kses２を、セッション鍵Kses１で暗号化させ、公開鍵モジュール１２１に送信する。公開鍵モジュール１２１の制御部６１は、暗号処理部３３の共通鍵処理部４２を制御して、受信したデータをセッション鍵Kses１で復号させることにより、セッション鍵Kses２を取り出す。

【０２５５】ステップS４５９において、図４８のステップＳ４１７と同様の処理が実行される。ステップＳ４６０において、公開鍵モジュール１２１の制御部６１は、移動するデータをセッション鍵Kses２で暗号化し、暗号化データをモジュール間通信用リーダライタ２－１３に送信する。

【０２５６】ステップＳ４６１において、図４９のステップＳ４４０と同様の処理が実行される。そして、ステップＳ４６２およびステップＳ４６３において、図４８のステップＳ４２２およびＳ４２３と同様の処理が実行される。

【０２５７】すなわち、図４８のステップＳ４２０およびステップＳ４２１においては、受信したデータをセッション鍵Kses１で復号し、復号したデータをセッション鍵Kses２で暗号化した後に共通鍵モジュール１２２に送信したが、ここでは、図４９を用いて説明した処理と同様に、共通鍵モジュール１２２と、公開鍵モジュール１２１とが、同一のセッション鍵Kses２を得ることができるため、これらの処理を行う必要がない。

【０２５８】そして、図５１のフローチャートを参照して、公開鍵モジュール１２１と共通鍵モジュール１２２が、共通秘密鍵K_commonを共有し、それを用いて相互認証を行い、更に、共通のセッション鍵Ksesを共有する場合の、モジュール間通信について説明する。

【０２５９】ステップＳ４７１およびステップＳ４７２において、公開鍵モジュール１２１と共通鍵モジュール１２２は、共通秘密鍵K_commonにより、相互認証を行い、セッション鍵Ksesを共有する。ステップＳ４７３において、モジュール間通信用リーダライタ２－１３は、ステップＳ４７１およびステップＳ４７２における相互認証の通信路のみ提供する（すなわち、公開鍵モジュール１２１とも共通鍵モジュール１２２とも、セッション鍵の共有は行われない）。

【０２６０】ステップＳ４７４において、図４８のステップＳ４１７と同様の処理が実行される。ステップＳ４７５において、公開鍵モジュール１２１の制御部６１は、暗号処理部３３の共通鍵処理部４２を制御して、移動するデータをセッション鍵Ksesで暗号化させ、暗号化データをモジュール間通信用リーダライタ２－１３に送信する。そして、ステップＳ４７６乃至ステップＳ４７８において、図４９のステップＳ４２１乃至ステップＳ４２３と同様の処理が実行される。

【０２６１】すなわち、図５１を用いて説明したモジュール間通信においては、モジュール間通信用リーダライタ２－１３は、データの通信路を提供するのみで、モジュール間通信されるデータを暗号化したり、復号することはない。

【０２６２】上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【０２６３】この記録媒体は、図９に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク１１５（フロッピー（登録商標）ディスクを含む）、光ディスク１１６（CD-ROM（Compact Disk-Read Only Memory），DVD（Digital Versatile Disk）を含む）、光磁気ディスク１１７（ＭＤ(Mini-Disk)を含む）、もしくは半導体メモリ１１８などよりなるパッケージメディアなどにより構成される。

【０２６４】また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２６５】

【発明の効果】本発明のデータ記憶装置、データ記憶方法、および記録媒体に記録されているプログラムによれば、情報処理装置に対するデータの入出力を制御し、複数のサービスに対応するデータの記憶を制御し、複数のサービスのうちの第１のサービスに対応する第１のサービスＩＤと、入出力制御ステップの処理により第１のサービスに関するデータの入出力が制御されている場合にデータの入出力が許可される、複数のサービスのうちの第２のサービスに対応する第２のサービスＩＤの記憶を制御するようにしたので、所定のサービスに関するデータの授受を実行している場合において、セキュリティを確保しつつ、予め許可された他のサービスに関するデー

タの授受を、並行して行うことを可能とすることができる。

【図面の簡単な説明】

【図１】ＩＣカードとリーダライタの通信方式および認証方式について説明するための図である。

【図２】カード発行者、サービス提供者、およびカード保持者の関係について説明するための図である。

【図３】ＩＣカードの構成を示すブロック図である。

【図４】ＩＣカードの構成を示すブロック図である。

【図５】図３および図４の暗号処理部について説明するための図である。

【図６】図３および図４のＳＲＡについて説明するための図である。

【図７】図６のＳＲＡに格納される認証用鍵情報について説明するための図である。

【図８】図３および図４のＳＲＴについて説明するための図である。

【図９】リーダライタの構成を示すブロック図である。

【図１０】サービス登録用リーダライタのメモリ情報を説明するための図である。

【図１１】一般リーダライタのメモリ情報を説明するための図である。

【図１２】モジュール間通信用リーダライタのメモリ情報を説明するための図である。

【図１３】モジュール間通信を説明するための図である。

【図１４】バージョンアップ用リーダライタのメモリ情報を説明するための図である。

【図１５】ＩＣカードとリーダライタの認証処理について説明するためのフローチャートである。

【図１６】リーダライタのサービス識別処理について説明するためのフローチャートである。

【図１７】ＩＣカードのサービス識別処理について説明するためのフローチャートである。

【図１８】リーダライタのサービス識別処理について説明するためのフローチャートである。

【図１９】ＩＣカードのサービス識別処理について説明するためのフローチャートである。

【図２０】リーダライタの認証鍵識別処理について説明するためのフローチャートである。

【図２１】ＩＣカードの認証鍵識別処理について説明するためのフローチャートである。

【図２２】リーダライタの認証鍵識別処理について説明するためのフローチャートである。

【図２３】ＩＣカードの認証鍵識別処理について説明するためのフローチャートである。

【図２４】証明書について説明するための図である。

【図２５】署名生成処理について説明するためのフローチャートである。

【図２６】署名検証処理について説明するためのフローチャートである。

【図２７】リーダライタの認証鍵識別処理について説明するためのフローチャートである。

【図２８】ＩＣカードの認証鍵識別処理について説明するためのフローチャートである。

【図２９】サービス登録用リーダライタのサービス登録処理について説明するためのフローチャートである。

【図３０】ＩＣカードのサービス登録処理について説明するためのフローチャートである。

【図３１】サービス登録用リーダライタのサービス削除処理について説明するためのフローチャートである。

【図３２】ＩＣカードのサービス削除処理について説明するためのフローチャートである。

【図３３】一般リーダライタのサービス削除処理について説明するためのフローチャートである。

【図３４】ＩＣカードのサービス削除処理について説明するためのフローチャートである。

【図３５】一般リーダライタのサービスデータ取得処理について説明するためのフローチャートである。

【図３６】ＩＣカードのサービスデータ送信処理について説明するためのフローチャートである。

【図３７】一般リーダライタのサービスデータ取得処理について説明するためのフローチャートである。

【図３８】ＩＣカードのサービスデータ送信処理について説明するためのフローチャートである。

【図３９】一般リーダライタのサービスデータ書き込み処理について説明するためのフローチャートである。

【図４０】ＩＣカードのサービスデータ書き込み処理について説明するためのフローチャートである。

【図４１】一般リーダライタのサービスデータ書き込み処理について説明するためのフローチャートである。

【図４２】ＩＣカードのサービスデータ書き込み処理について説明するためのフローチャートである。

【図４３】バージョンアップ用リーダライタの鍵バージョンアップ処理について説明するためのフローチャートである。

【図４４】ＩＣカードの鍵バージョンアップ処理について説明するためのフローチャートである。

【図４５】一般リーダライタの鍵バージョンアップ処理について説明するためのフローチャートである。

【図４６】ＩＣカードの鍵バージョンアップ処理について説明するためのフローチャートである。

【図４７】ＩＣカードの鍵バージョンアップ処理について説明するためのフローチャートである。

【図４８】モジュール間通信処理について説明するためのフローチャートである。

【図４９】モジュール間通信処理について説明するためのフローチャートである。

【図５０】モジュール間通信処理について説明するためのフローチャートである。

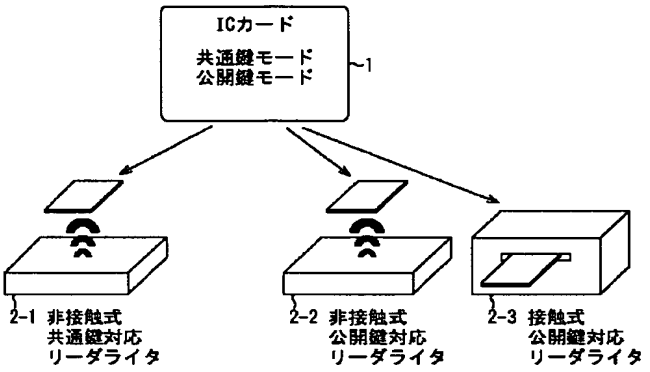
45　　46

【図５１】モジュール間通信処理について説明するためのフローチャートである。

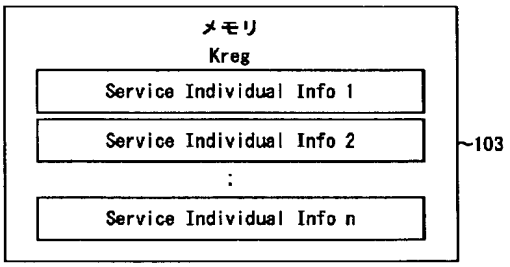
【符号の説明】

１　ＩＣカード１　リーダライタ、　２１　通信部、　３１　制御部、　３２メモリ、　３３　暗号処理部、　４１　公開鍵処理部、　４２　共通鍵処理部、　４３　その他の暗号処理部、　４５　ＳＲＴ、　４６　ＳＲＡ、　５１　通信部、　５２　共通鍵サービス処理部、＊　５３　通信部、　５４　公開鍵サービス処理部、　６１　制御部、　６２　メモリ、６３　暗号処理部、　９１　通信部、　１０１　制御部、　１０２　暗号処理部、　１０３　メモリ、　１１１公開鍵処理部、　１１２　共通鍵処理部、　１１３　その他の暗号処理部、　１０５　表示部、　１０６　入力部、　１２１　公開鍵モジュール、　１２２　共通鍵モジュール

【図１】

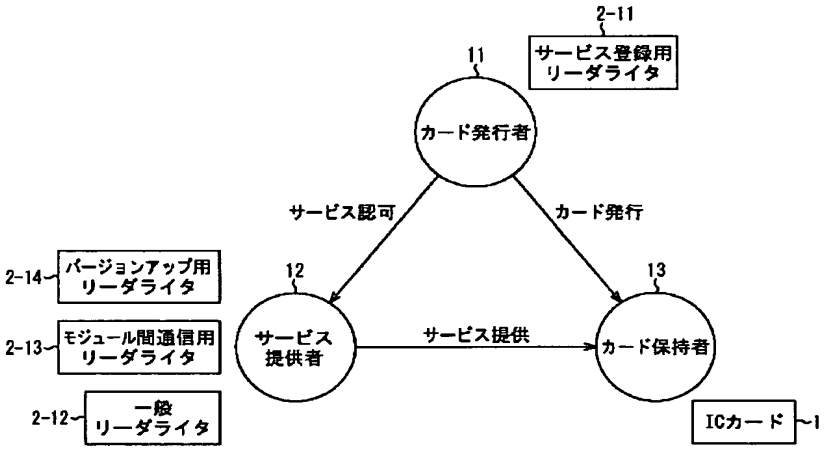


【図１０】

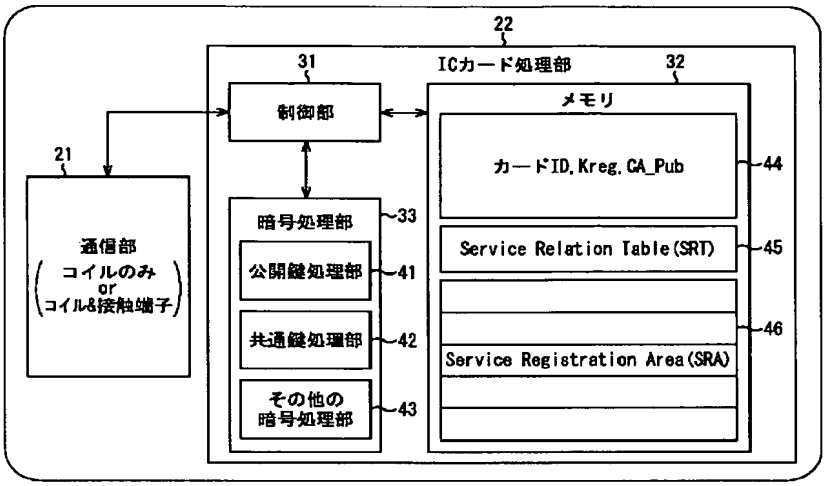


サービス登録用リーダライタ2-11のメモリ情報

【図２】

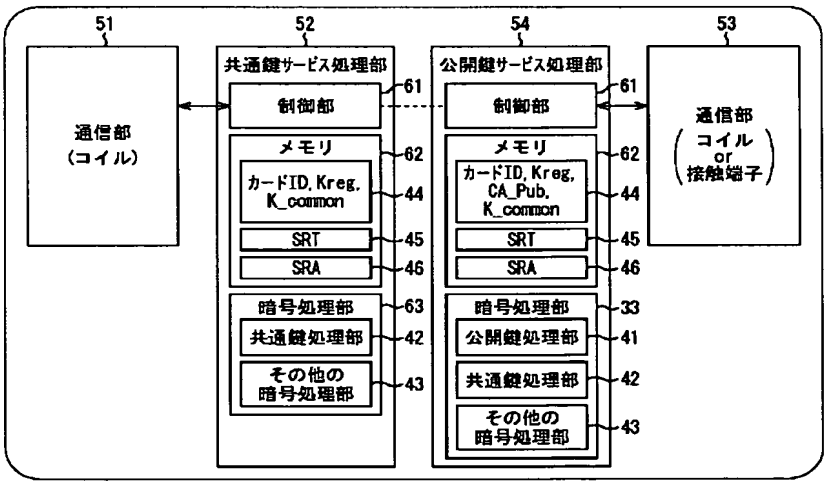


【図３】



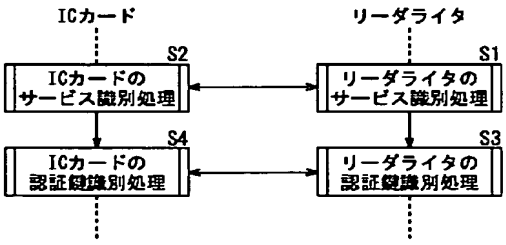
ICカード 1

【図４】

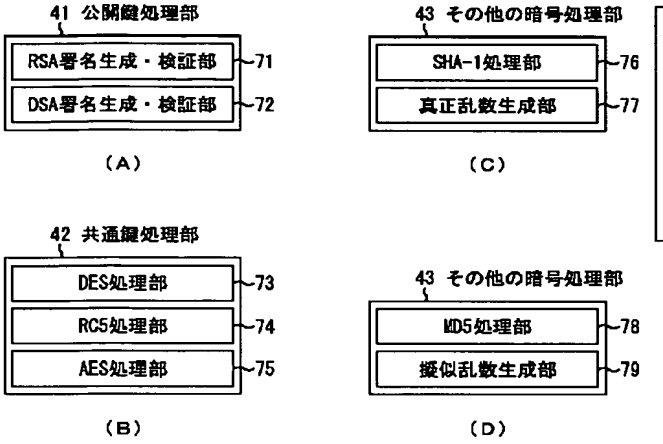


ICカード 1

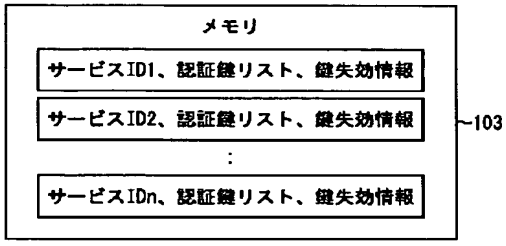
【図１５】



【図５】

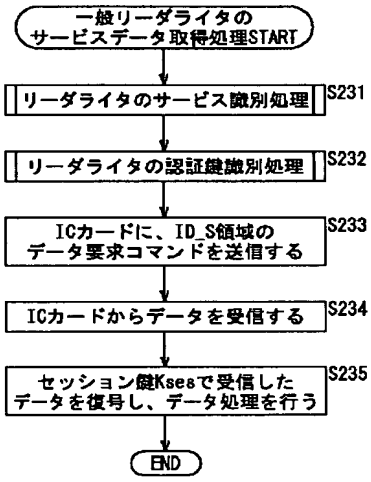


【図１１】

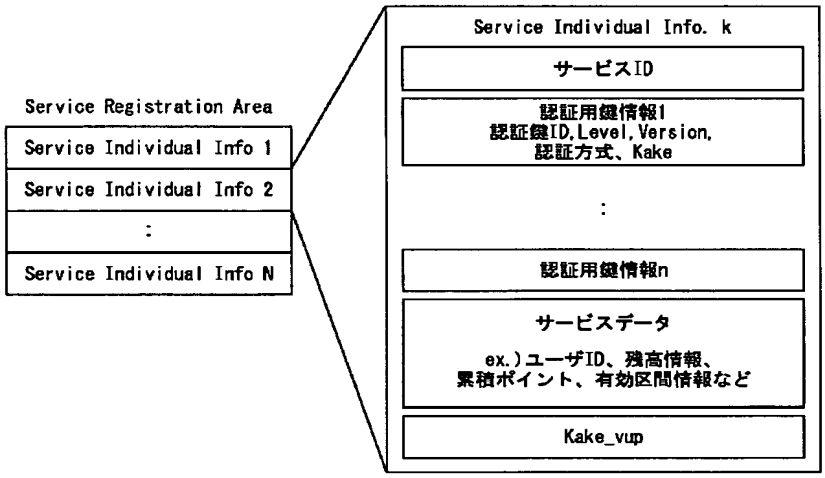


一般リーダライタ2-12のメモリ情報

【図３５】

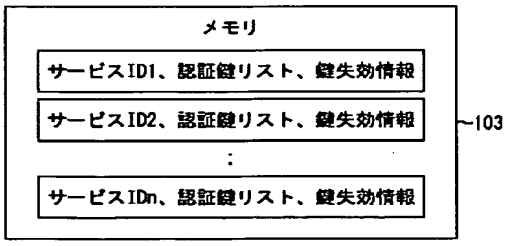


【図６】



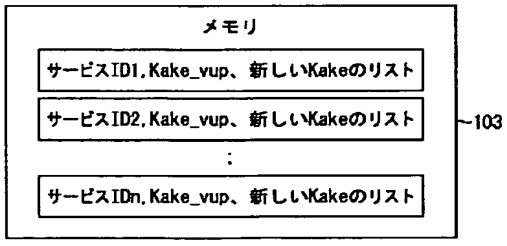
SRAに格納されている情報

【図１２】



モジュール間通信用リーダライタ 2-13のメモリ情報

【図１４】



バージョンアップ用リーダライタ 2-14のメモリ情報

【図７】

(A)

共通鍵・公開鍵の2種類の認証鍵格納状態

領域No.	認証鍵ID	Version	認証方式	Kake	Certificate
1	0005	3	共、DES56bit	0100...01	None
2	0018	2	公、ECC128bit	0110...11	証明書データ

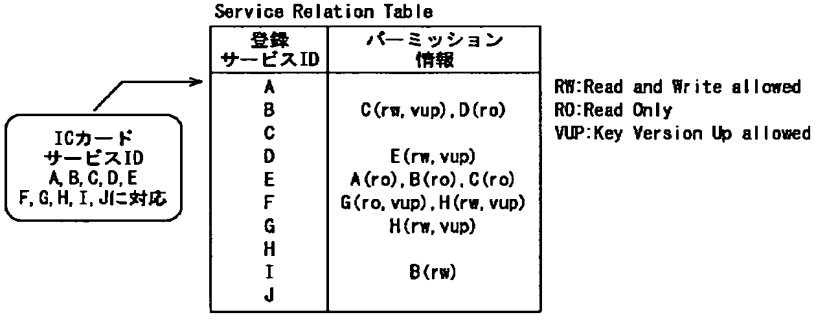
(B)

複数レベルの鍵格納状態

領域No.	認証鍵ID	Level	Version	認証方式	Kake	Certificate
1	0005	1	3	共、DES56bit	0100...01	None
2	0018	5	2	共、AES128bit	0110...11	None
3	0434	3	1	公、RSA512bit	0011...10	証明書データ
4	0124	6	6	公、RSA2048bit	1011...01	証明書データ
5	0855	2	4	共、AES256bit	1001...00	None
6	0435	4	1	公、ECC160bit	1110...11	証明書データ
7	0342	7	1	公、ECC224bit	0101...10	証明書データ

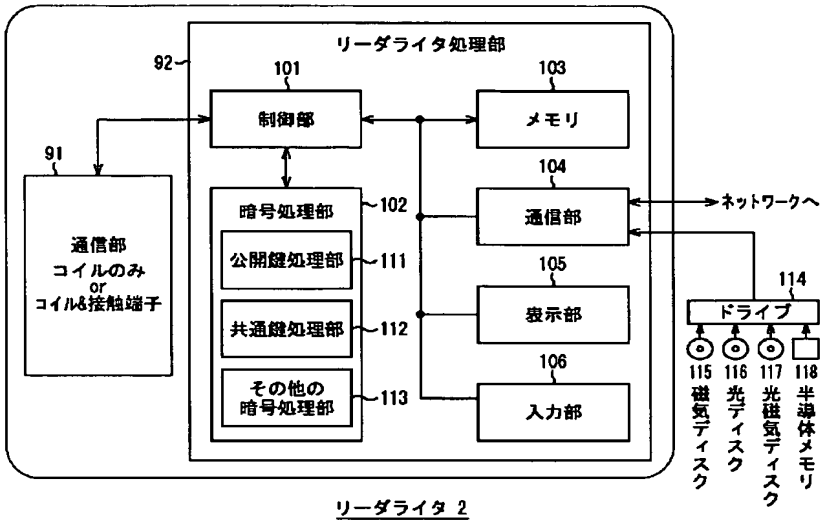
認証用鍵情報

【図８】



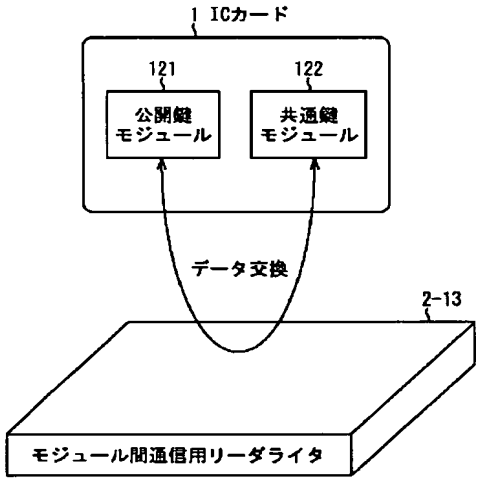
Service Relation Tableに格納されている情報

【図９】



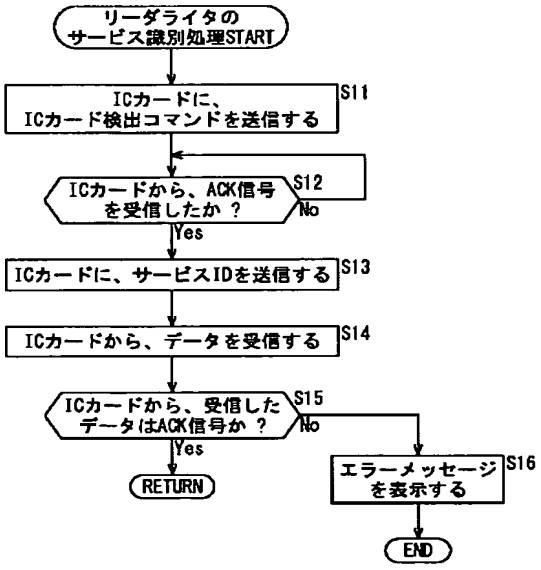
リーダライタ 2

【図１３】

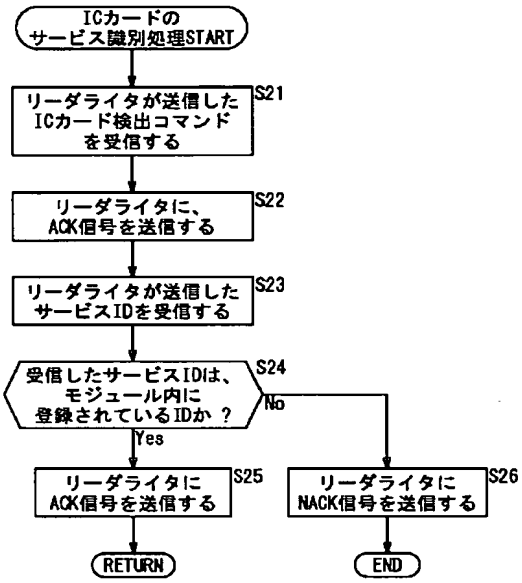


モジュール間通信

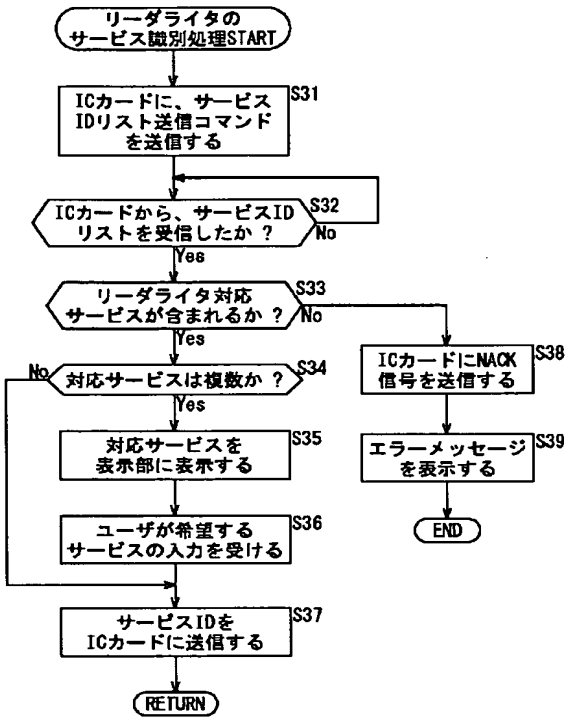
【図１６】



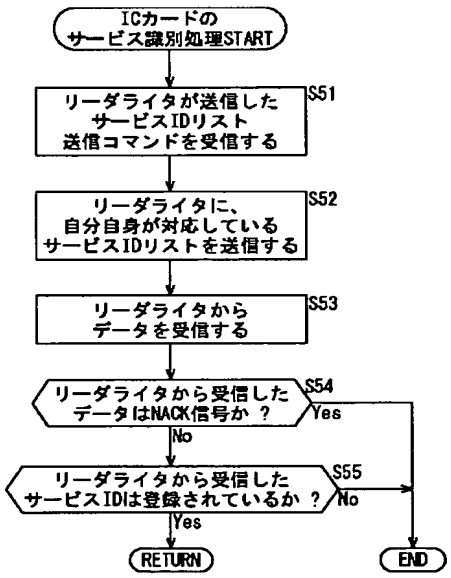
【図１７】



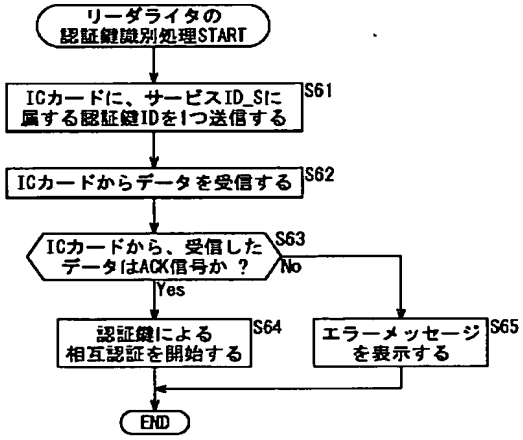
【図１８】



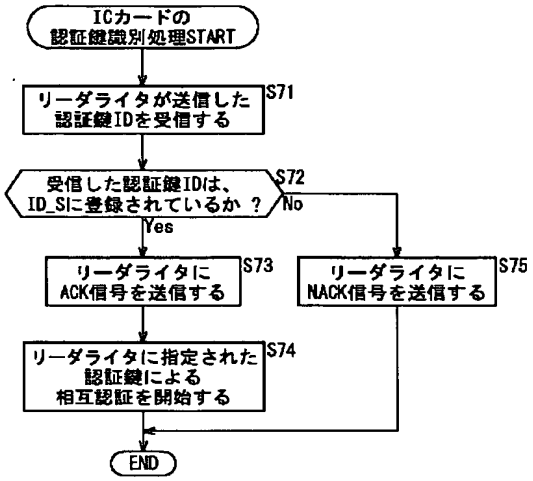
【図１９】



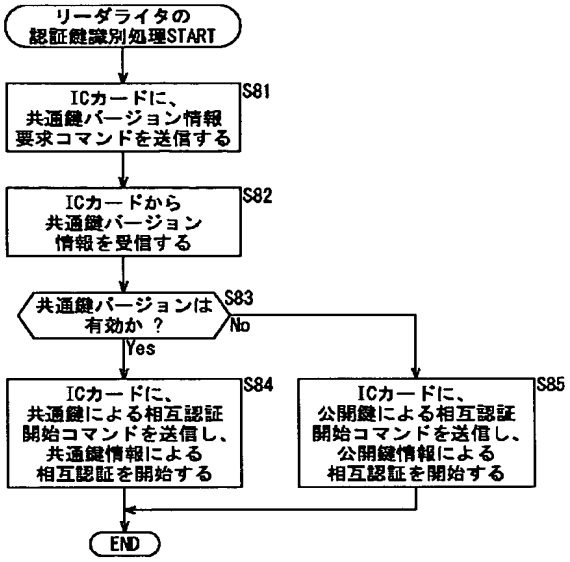
【図２０】



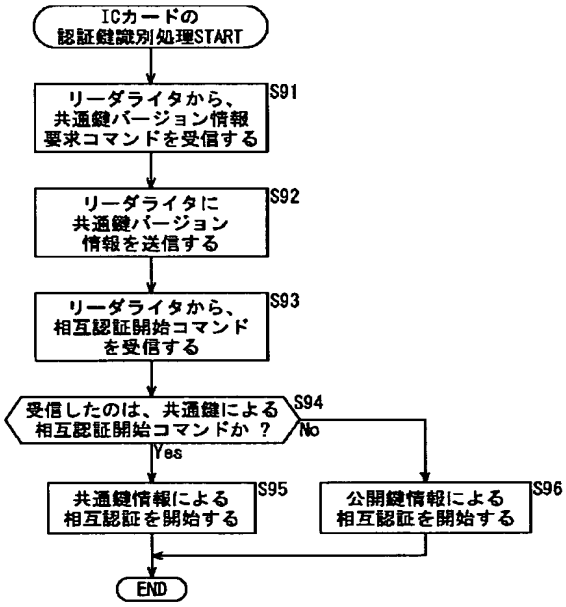
【図２１】



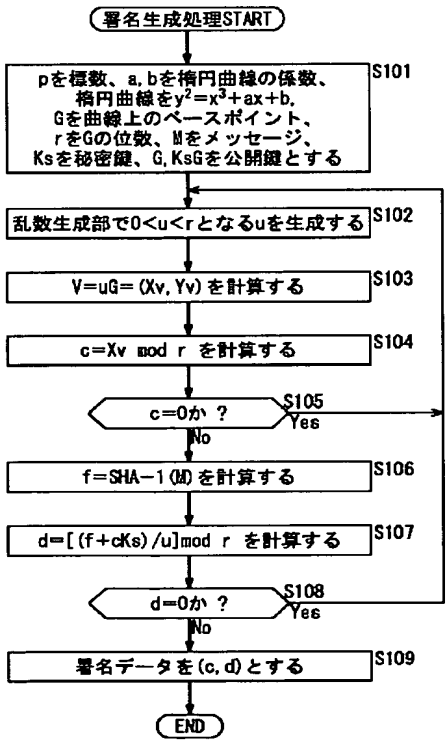
【図２２】



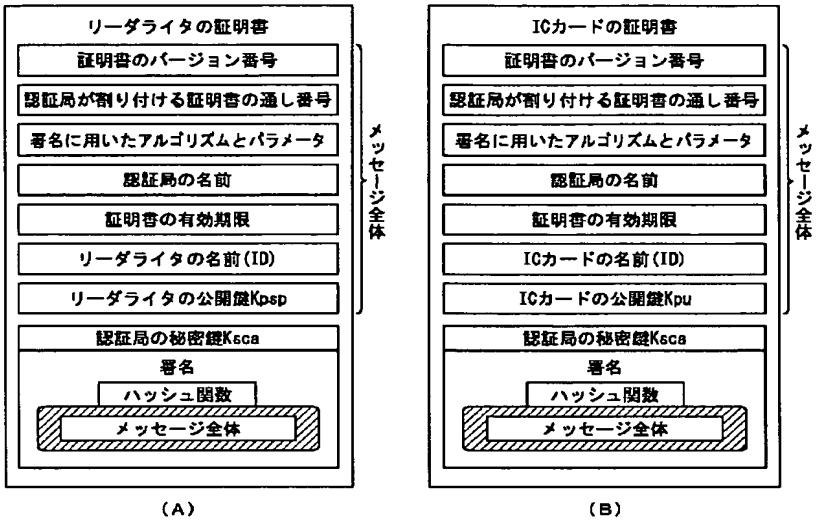
【図２３】



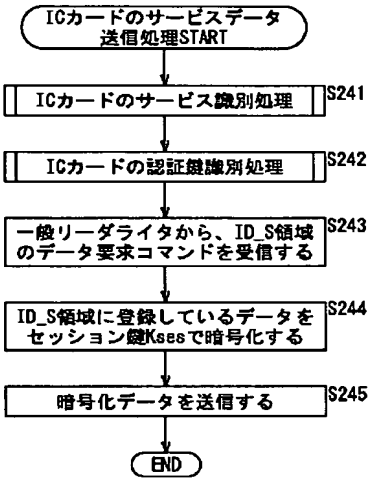
【図２５】



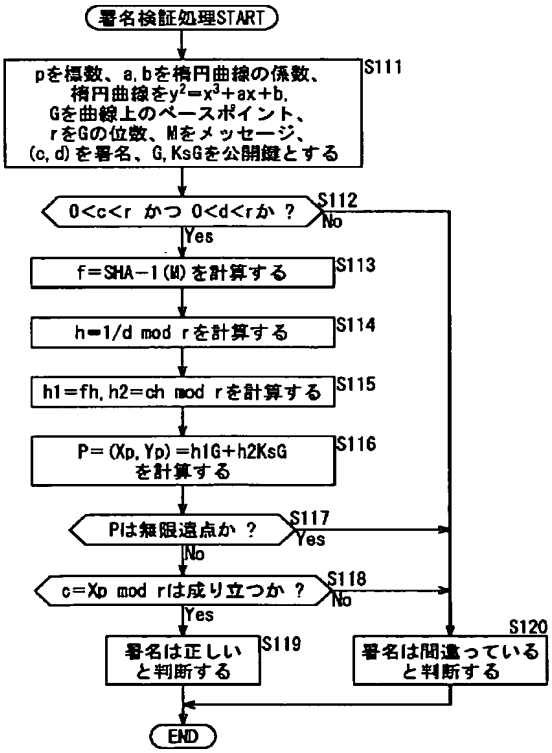
【図２４】



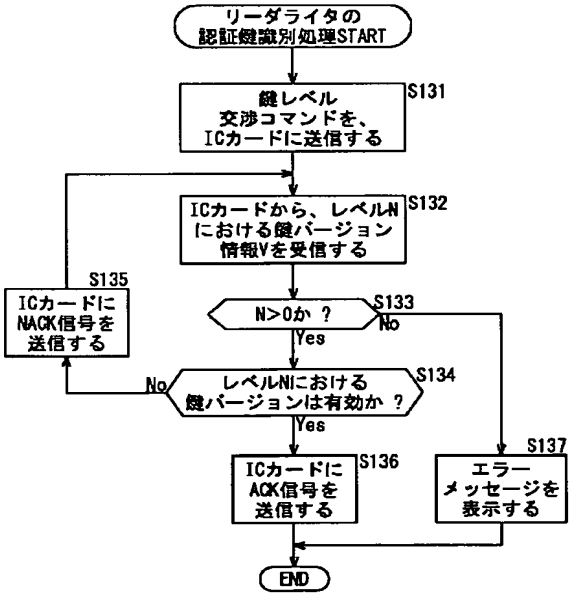
【図３６】



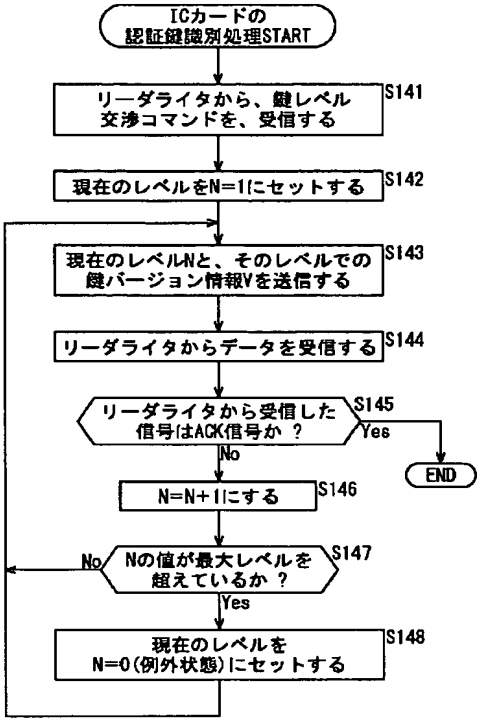
【図２６】



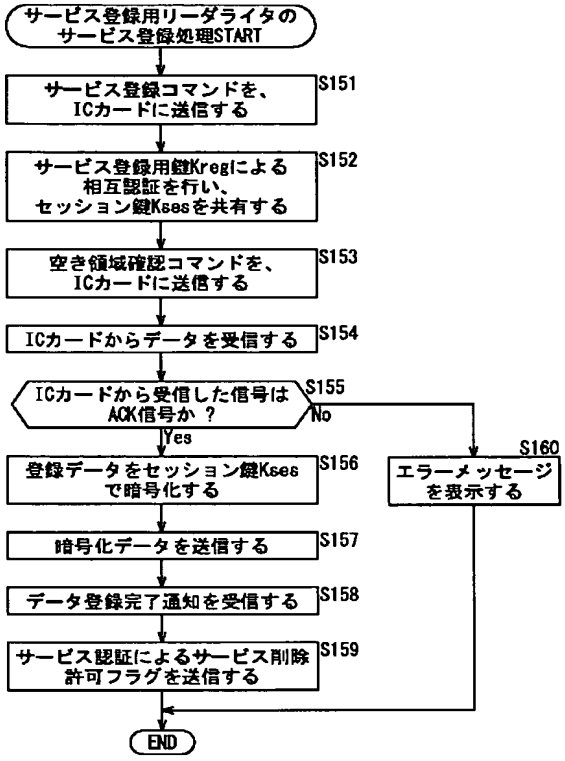
【図２７】



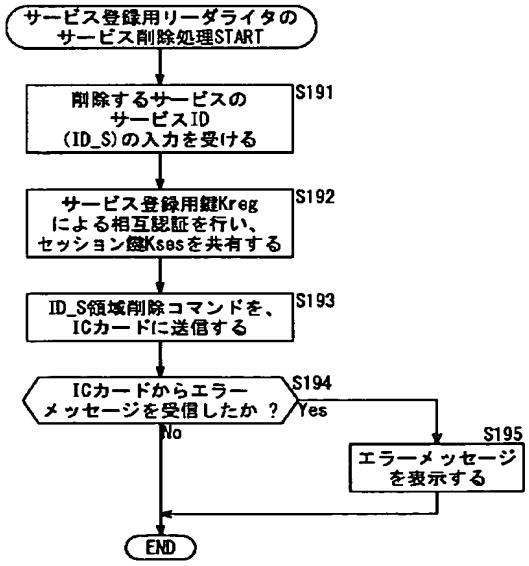
【図２８】



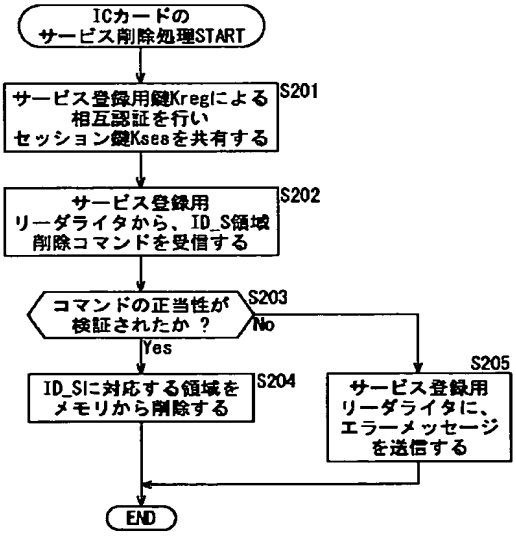
【図２９】



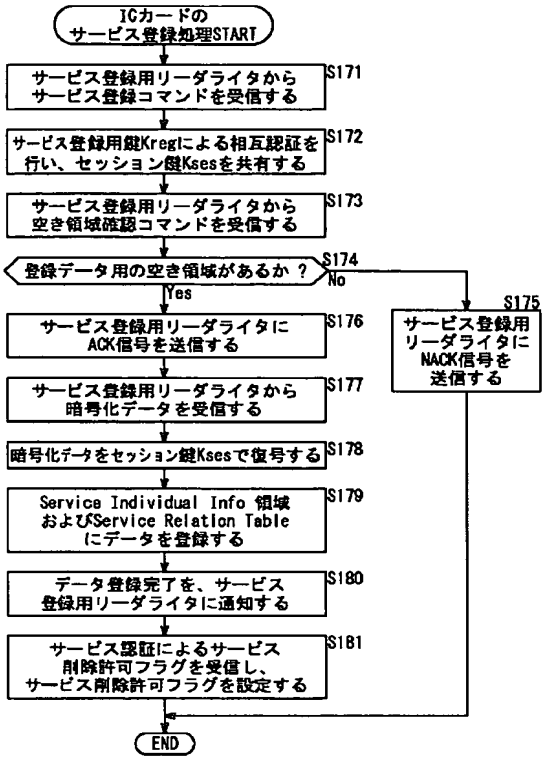
【図３１】



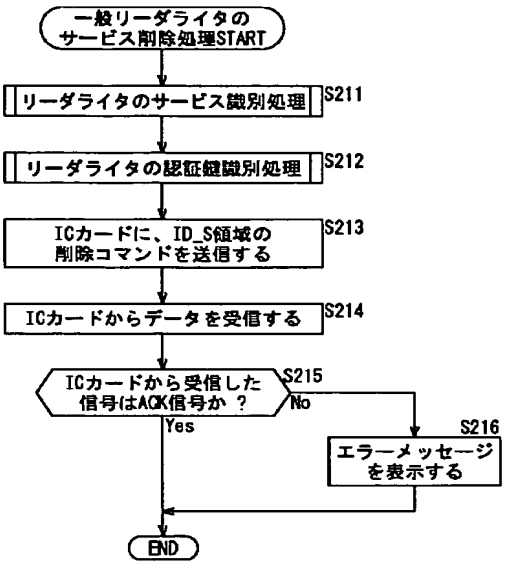
【図３２】



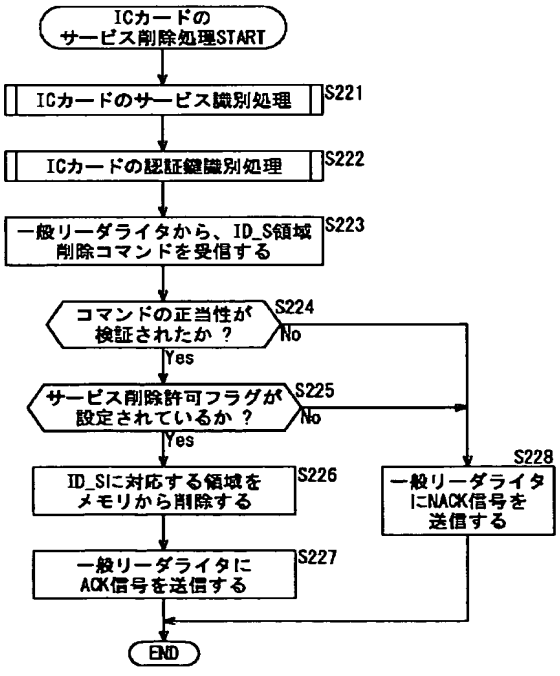
【図３０】



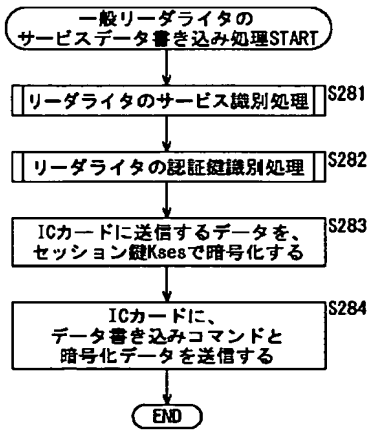
【図３３】



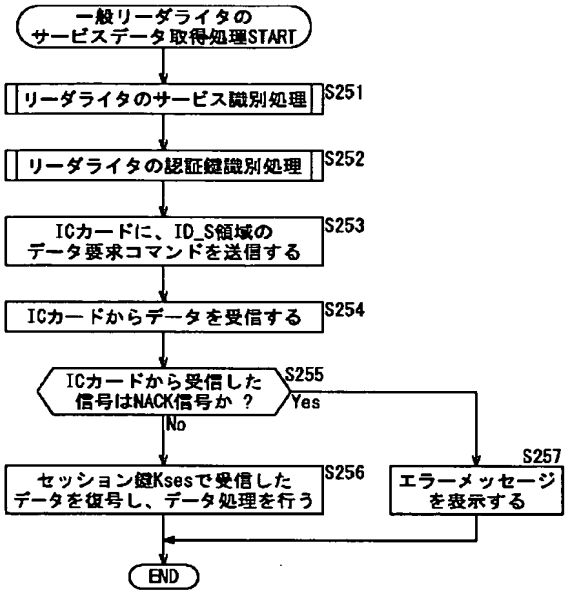
【図３４】



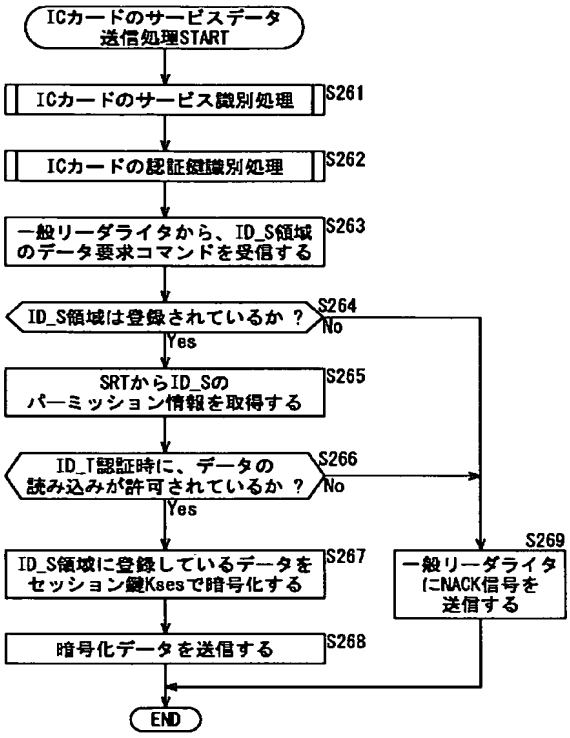
【図３９】



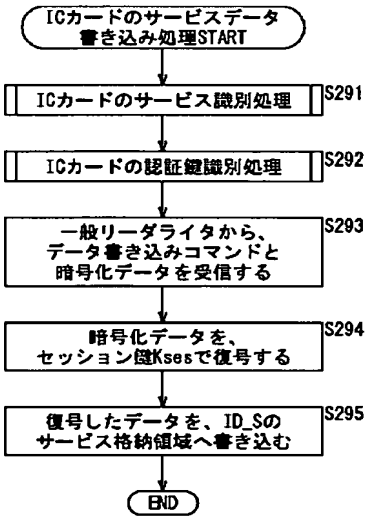
【図３７】



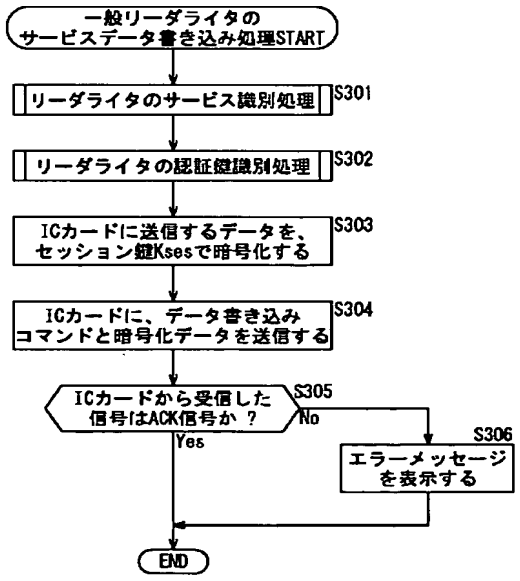
【図３８】



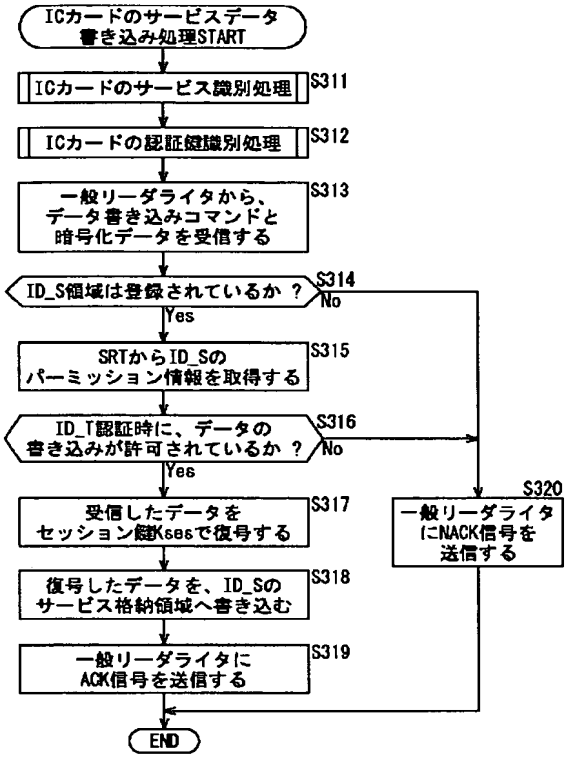
【図４０】



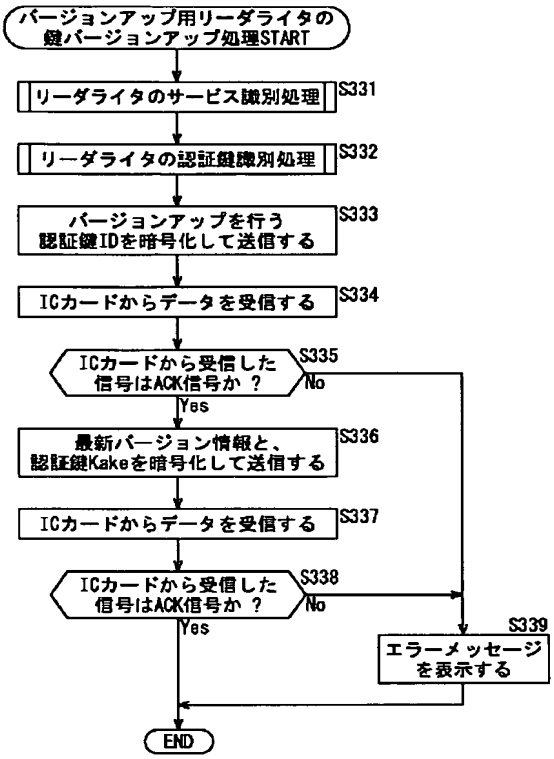
【図４１】



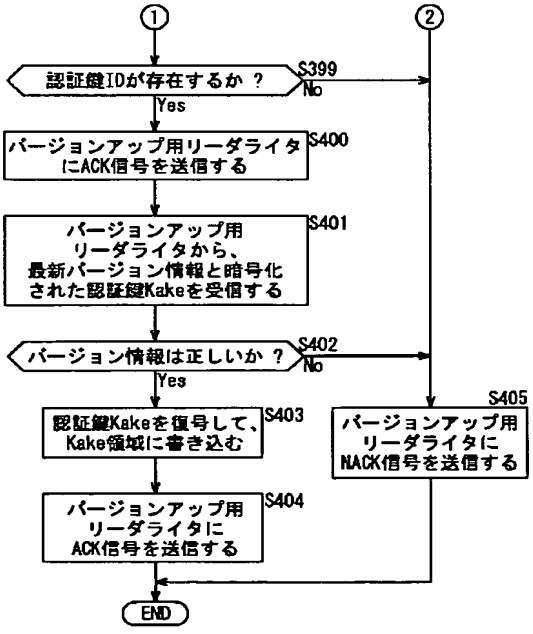
【図４２】


ICカードのサービスデータ
書き込み処理START
ICカードのサービス識別処理
S311
ICカードの認証鍵識別処理
S312
一般リーダライタから、
データ書き込みコマンドと
暗号化データを受信する
S313
ID_S領域は登録されているか ？
S314
No
Yes
SRTからID_Sの
パーミッション情報を取得する
S315
ID_T認証時に、データの
書き込みが許可されているか ？
S316
No
Yes
受信したデータを
セッション鍵Ksesで復号する
S317
復号したデータを、ID_Sの
サービス格納領域へ書き込む
S318
一般リーダライタに
ACK信号を送信する
S319
一般リーダライタ
にNACK信号を
送信する
S320
END

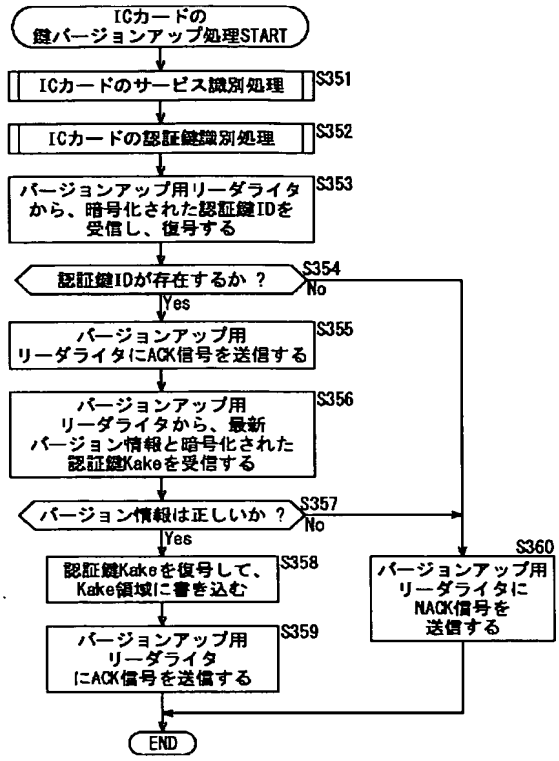
【図４３】


バージョンアップ用リーダライタの
鍵バージョンアップ処理START
リーダライタのサービス識別処理
S331
リーダライタの認証鍵識別処理
S332
バージョンアップを行う
認証鍵IDを暗号化して送信する
S333
ICカードからデータを受信する
S334
ICカードから受信した
信号はACK信号か ？
S335
No
Yes
最新バージョン情報と、
認証鍵Kakeを暗号化して送信する
S336
ICカードからデータを受信する
S337
ICカードから受信した
信号はACK信号か ？
S338
No
Yes
エラーメッセージ
を表示する
S339
END

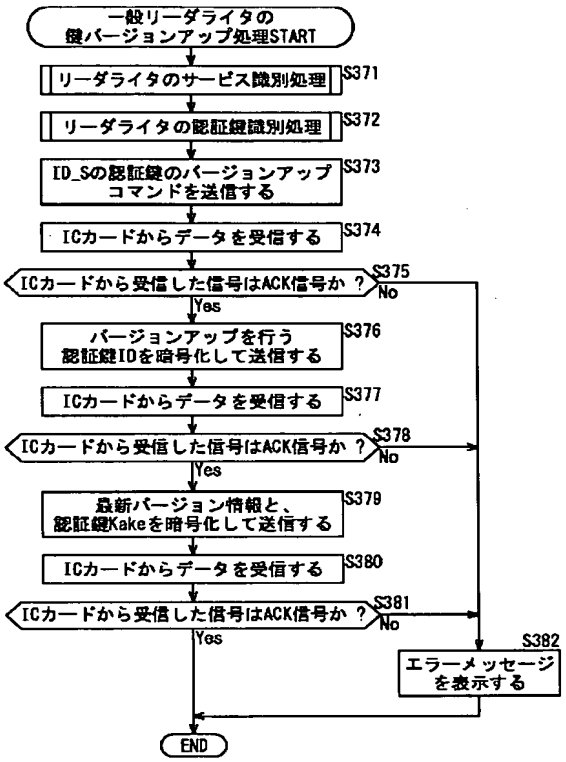
【図４７】


①
②
認証鍵IDが存在するか ？
S399
No
Yes
バージョンアップ用リーダライタ
にACK信号を送信する
S400
バージョンアップ用
リーダライタから、
最新バージョン情報と暗号化
された認証鍵Kakeを受信する
S401
バージョン情報は正しいか ？
S402
No
Yes
認証鍵Kakeを復号して、
Kake領域に書き込む
S403
バージョンアップ用
リーダライタに
ACK信号を送信する
S404
バージョンアップ用
リーダライタに
NACK信号を送信する
S405
END

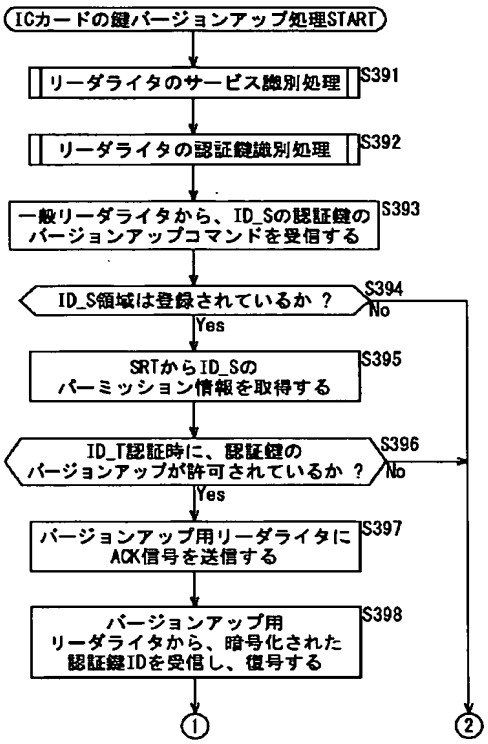
【図４４】


ICカードの
鍵バージョンアップ処理START
ICカードのサービス識別処理
S351
ICカードの認証鍵識別処理
S352
バージョンアップ用リーダライタから、暗号化された認証鍵IDを受信し、復号する
S353
認証鍵IDが存在するか ？
S354
No
Yes
バージョンアップ用リーダライタにACK信号を送信する
S355
バージョンアップ用リーダライタから、最新バージョン情報と暗号化された認証鍵Kakeを受信する
S356
バージョン情報は正しいか ？
S357
No
Yes
認証鍵Kakeを復号して、Kake領域に書き込む
S358
バージョンアップ用リーダライタにACK信号を送信する
S359
バージョンアップ用リーダライタにNACK信号を送信する
S360
END

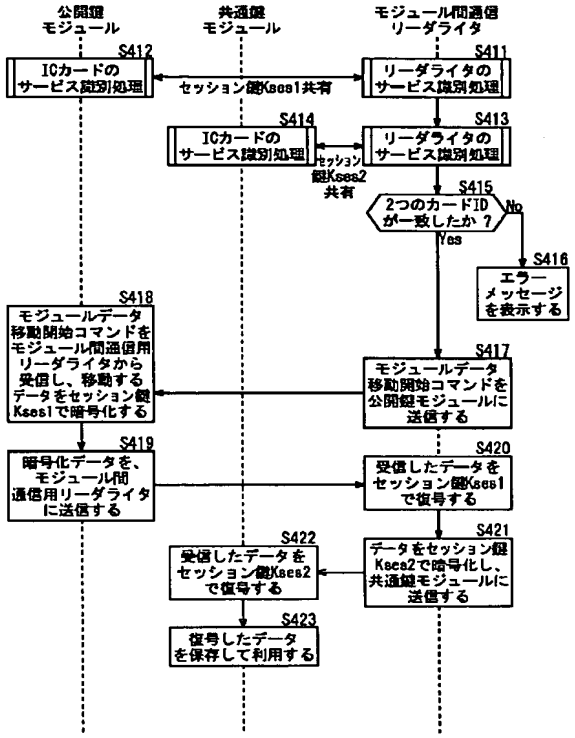
【図４５】


一般リーダライタの
鍵バージョンアップ処理START
リーダライタのサービス識別処理
S371
リーダライタの認証鍵識別処理
S372
ID_Sの認証鍵のバージョンアップコマンドを送信する
S373
ICカードからデータを受信する
S374
ICカードから受信した信号はACK信号か ？
S375
No
Yes
バージョンアップを行う認証鍵IDを暗号化して送信する
S376
ICカードからデータを受信する
S377
ICカードから受信した信号はACK信号か ？
S378
No
Yes
最新バージョン情報と、認証鍵Kakeを暗号化して送信する
S379
ICカードからデータを受信する
S380
ICカードから受信した信号はACK信号か ？
S381
No
Yes
エラーメッセージを表示する
S382
END

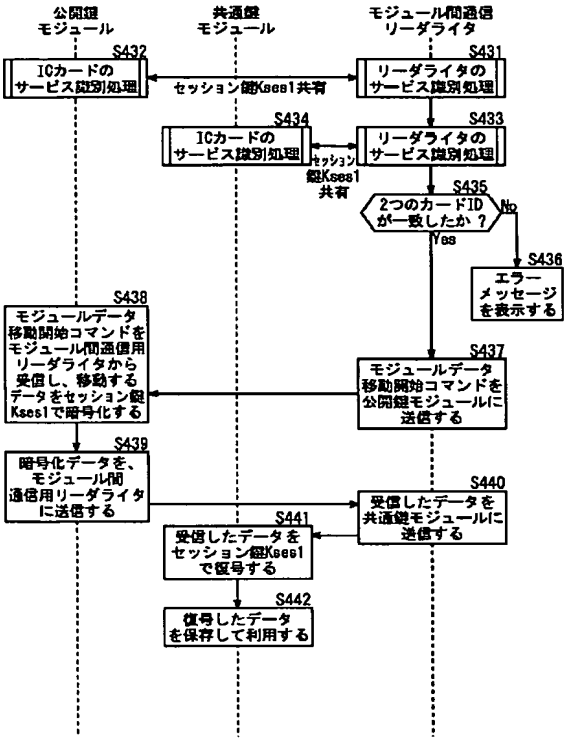
【図４６】


ICカードの鍵バージョンアップ処理START
リーダライタのサービス識別処理
S391
リーダライタの認証鍵識別処理
S392
一般リーダライタから、ID_Sの認証鍵のバージョンアップコマンドを受信する
S393
ID_S領域は登録されているか ？
S394
No
Yes
SRTからID_Sのパーミッション情報を取得する
S395
ID_T認証時に、認証鍵のバージョンアップが許可されているか ？
S396
No
Yes
バージョンアップ用リーダライタにACK信号を送信する
S397
バージョンアップ用リーダライタから、暗号化された認証鍵IDを受信し、復号する
S398
①
②

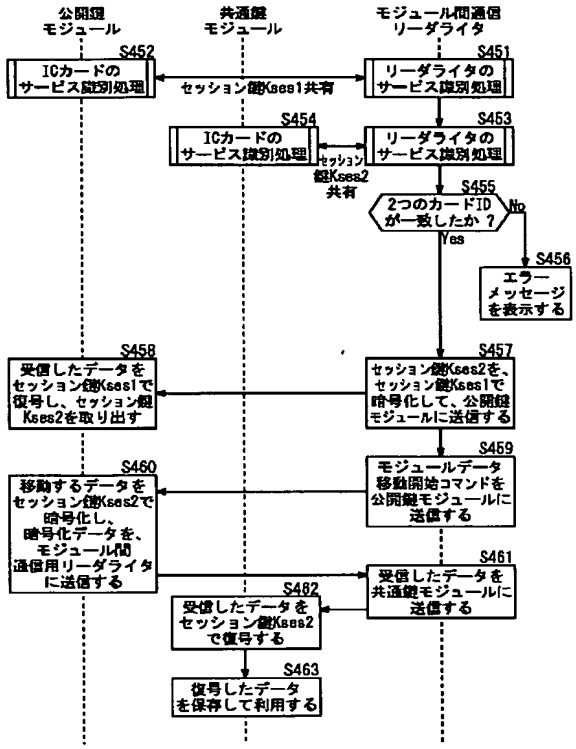
【図４８】


公開鍵モジュール
共通鍵モジュール
モジュール間通信リーダライタ
S412
ICカードのサービス識別処理
セッション鍵Kses1共有
S411
リーダライタのサービス識別処理
S414
ICカードのサービス識別処理
セッション鍵Kses2共有
S413
リーダライタのサービス識別処理
S415
2つのカードIDが一致したか ？
No
Yes
S416
エラーメッセージを表示する
S418
モジュールデータ移動開始コマンドをモジュール間通信用リーダライタから受信し、移動するデータをセッション鍵Kses1で暗号化する
S417
モジュールデータ移動開始コマンドを公開鍵モジュールに送信する
S419
暗号化データを、モジュール間通信用リーダライタに送信する
S420
受信したデータをセッション鍵Kses1で復号する
S422
受信したデータをセッション鍵Kses2で復号する
S421
データをセッション鍵Kses2で暗号化し、共通鍵モジュールに送信する
S423
復号したデータを保存して利用する

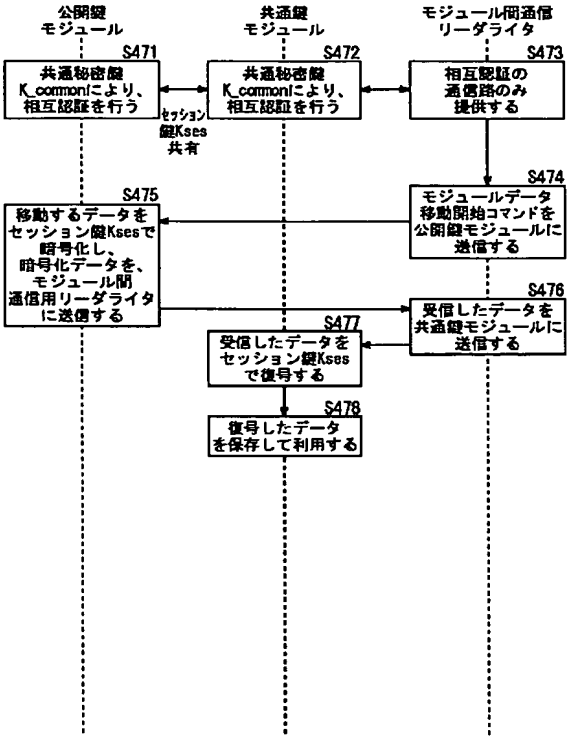
【図４９】


公開鍵モジュール
共通鍵モジュール
モジュール間通信リーダライタ
S432
ICカードのサービス識別処理
セッション鍵Kses1共有
S431
リーダライタのサービス識別処理
S434
ICカードのサービス識別処理
セッション鍵Kses1共有
S433
リーダライタのサービス識別処理
S435
2つのカードIDが一致したか？
No
Yes
S436
エラーメッセージを表示する
S438
モジュールデータ移動開始コマンドをモジュール間通信用リーダライタから受信し、移動するデータをセッション鍵Kses1で暗号化する
S437
モジュールデータ移動開始コマンドを公開鍵モジュールに送信する
S439
暗号化データを、モジュール間通信用リーダライタに送信する
S440
受信したデータを共通鍵モジュールに送信する
S441
受信したデータをセッション鍵Kses1で復号する
S442
復号したデータを保存して利用する

【図５０】


公開鍵モジュール
共通鍵モジュール
モジュール間通信リーダライタ
S452
ICカードのサービス識別処理
セッション鍵Kses1共有
S451
リーダライタのサービス識別処理
S454
ICカードのサービス識別処理
セッション鍵Kses2共有
S453
リーダライタのサービス識別処理
S455
2つのカードIDが一致したか？
No
Yes
S456
エラーメッセージを表示する
S458
受信したデータをセッション鍵Kses1で復号し、セッション鍵Kses2を取り出す
S457
セッション鍵Kses2を、セッション鍵Kses1で暗号化して、公開鍵モジュールに送信する
S460
移動するデータをセッション鍵Kses2で暗号化し、暗号化データを、モジュール間通信用リーダライタに送信する
S459
モジュールデータ移動開始コマンドを公開鍵モジュールに送信する
S461
受信したデータを共通鍵モジュールに送信する
S462
受信したデータをセッション鍵Kses2で復号する
S463
復号したデータを保存して利用する

【図５１】



フロントページの続き

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　吉野　賢治
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　瀧　隆太
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B035 AA13 BB09 BC02 CA23
5B058 CA15 KA11 KA33 KA35 YA06
5J104 AA07 KA01 NA35 NA36 NA38
NA41